УНИВЕРСИТЕТ ИТМО

С.М. Платунова

АДМИНИСТРИРОВАНИЕ СЕТИ В WINDOWS SERVER 2012

Учебное пособие

Санкт-Петербург

2015

Платунова С.М. Администрирование сети Winsows Server 2012. Учебное пособие по дисциплине «Администрирование вычислительных сетей». – СПб: НИУ ИТМО, 2015. – 102 с.

В учебном пособии содержатся основные сведения об администрировании сети под управлением операционной системы Microsoft Windows Server 2012, такие как: Управление TCP/IP-сетью, запуск DCHP-клиентов и серверов, оптимизация DNS.

Пособие адресовано специалистам с высшим и средним профессиональным образованием, имеющим опыт работы в области IT технологий, обучающихся по направлению/специальности: 09.04.01 «Информатика и вычислительная техника» («Системное администрирование аппаратно-программных комплексов»)

Рекомендовано к печати Ученым советом факультета Академии ЛИМТУ, протокол № 5 от 06.11.2014

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

ГЛАВА 1 Управление TCP/IP-сетью

Администратор разрешает компьютерам взаимодействовать по сети, используя базовые сетевые протоколы, встроенные в Windows Server 2012. Основным сетевым протоколом является TCP/IP. Протокол TCP/IP — это набор протоколов и служб, используемых для сетевого взаимодействия, и основной протокол для межсетевого взаимодействия. По сравнению с другими сетевыми протоколами настройка TCP/IP довольно сложна, зато TCP/IP — самый универсальный протокол.

Настройки групповой политики могут влиять на возможность устанавливать и управлять TCP/IP-сетью. Ключевые политики, которые необходимо исследовать, находятся в узлах Конфигурация пользователя\Административные шаблоны\Сеть\Сетевые подключения (User Configuration\Administrative Templates\Network\Network Connections) и Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy). Навигация по сетям в Windows Server 2012

В Windows Server 2012 имеется расширенный набор сетевых утилит:

- Обозреватель сети (Network Explorer) — предоставляет собой основное средство просмотра компьютеров и устройств сети;
- Центр управления сетями и общим доступом (Network and Sharing Center) — основная консоль для просмотра и управления конфигурацией сети и общего доступа;
- Диагностика сети (Network Diagnostics) — предоставляет средство автоматической ди- агностики для обнаружения и решения сетевых проблем.

Перед описанием этих утилит посмотрим на компоненты Windows Server 2012, на которых и основаны эти утилиты:

- Сетевое обнаружение (Network Discovery) — компонент Windows Server 2012, управляющий способностью видеть другие компьютеры и устройства;
- Служба сетевого расположения (Network Awareness) — компонент Windows Server 2012, уведомляющий об изменениях в подключениях узлов и конфигурации сети.

Компьютеры под управлением Windows Vista с SP1 или более поздние версии Windows поддерживают расширения сетевого расположения. Эти расположения позволяют компьютеру подключаться к одному или нескольким сетям через два или более интерфейса (независимо от типа соединения — проводное или беспроводное) для выбора маршрута с лучшей производительностью для передачи данных. В рамках выбора лучшего маршрута Windows выбирает лучший интерфейс (проводной или

беспроводной) для передачи. Этот механизм улучшает выбор беспроводного интерфейса по проводным сетям, когда оба интерфейса присутствуют.

Параметры сетевого обнаружения используемого компьютера определяют, какие компьютеры и устройства будут доступны в сетевых инструментах Windows Server 2012. Параметры обнаружения работают в сочетании с Брандмауэром Windows и способны блокировать или разрешать следующие действия:

- обнаружение сетевых компьютеров и устройств;
- обнаружение компьютера другими системами.

Параметры сетевого обнаружения должны обеспечить надлежащий уровень безопасности для каждой из категорий сетей, к которым подключен компьютер. Существуют три категории сетей:

- доменная сеть — сеть, в которой компьютеры подключены к домену предприятия;
- частная сеть — сеть, компьютеры которой являются членами рабочей группы и лишены прямого выхода в Интернет;
- публичная сеть — сеть в общественном месте, например, в кафе или аэропорту.

Поскольку компьютер хранит настройки отдельно для каждой категории сети, различные настройки блокирования и разрешения могут использоваться для каждой категории. При первом подключении сетевого адаптера компьютера к сети Windows устанавливает категорию сети на основании конфигурации компьютера. Основываясь на категории сети, ОС Windows Server 2012 автоматически настраивает параметры, которые могут включать или выключать обнаружение. Если режим обнаружения включен, то:

- компьютер может обнаруживать другие компьютеры и устройства в сети;
- другие компьютеры и устройства в сети могут обнаруживать этот компьютер.

Когда обнаружение выключено, то:

- компьютер не способен обнаруживать другие компьютеры и устройства в сети;
- другие компьютеры и устройства в сети не могут обнаруживать этот компьютер.

Обычно сетевой адаптер устанавливается как публичный, прежде чем компьютер будет подключен к домену. Обозреватель сети отображает список обнаруженных компьютеров и устройств в сети. Для доступа к обозревателю сети запустите Проводник на экране Пуск (Start). В окне Проводника выберите Сеть (Network) на панели слева.

Какие компьютеры и устройства будут отображены в обозревателе сети, зависит от настроек сетевого обнаружения компьютера, операционной системы и от того, является ли компьютер членом домена. Если обнаружение блокируется, и сервер под управлением Windows Server 2012 не является членом домена, будет отображено соответствующее предупреждение. Щелкните на этом предупреждении и выберите команду Включить сетевое обнаружение (Turn On Network Discovery And File Sharing), чтобы включить сетевое обнаружение. В результате будут открыты соответствующие порты Брандмауэра Windows.

Центр управления сетями и общим доступом (Network and Sharing Center), предоставляет информацию о текущем состоянии сети, а также обзор текущей конфигурации сети. Чтобы открыть Центр управления сетями и общим доступом в Панели щелкните по ссылке Просмотр состояния сети и задач (View network status and tasks) под заголовком Сеть и Интернет (Network and Internet).

Центр управления сетями и общим доступом предоставляет обзор сети. Под именем сети выводится ее категория, например Доменная сеть (Domain network), Частная сеть (Private network) или Общедоступная сеть (Public network). Поле Тип доступа (Access type) указывает, как компьютер подключен к текущей сети. Значения для этой опции могут быть следующими: Без доступа к сети (No network access), Без доступа к Интернету (No Internet access) или Интернет (Internet). При щелчке по имени подключения можно будет увидеть соответствующее окно состояния.

Щелкните на задаче Изменение параметров адаптера (Change adapter settings) для отображения страницы Сетевые подключения (Network Connections), которая используется для управления сетевыми подключениями. Щелчок на задаче Изменить дополнительные параметры общего доступа (Change advanced sharing settings) предоставляет возможность настройки параметров общего доступа и сетевого обнаружения для каждого профиля сети.

Для управления профилем разверните панель профиля, нажав кнопку со стрелкой вниз напротив имени профиля, установите параметры, а затем нажмите кнопку Сохранить изменения (Save changes). Чтобы включить или выключить сетевое обнаружение, выберите, соответственно, Включить сетевое обнаружение (Turn on network discovery) или Отключить сетевое обнаружение (Turn off network discovery), а затем нажмите кнопку Сохранить изменения1.

Средствами Центра управления сетями и общим доступом можно диагностировать проблемы с сетью. Для этого щелкните на ссылке Устранение неполадок (Troubleshoot problems) и выберите возникшую проблему, например Входящие подключения (Incoming Connections), а

затем следуйте инструкциям. Диагностика сети попытается идентифицировать проблему и предложит возможное решение.

Управление сетью в Windows 8 и Windows Server 2012

В групповой политике находятся политики управления сетью как для проводных сетей (IEEE 802.3), так и для беспроводных сетей (IEEE 802.11). Эти политики находятся в узле Конфигурация компьютера\Конфигурация Windows\Параметры безопасности (Computer Configuration\Windows Settings\Security Settings). Только одна проводная и одна беспроводная политики могут быть созданы и применены за один раз. Это означает, что можно устанавливать как проводные, так и беспроводные политики для компьютеров под управлением Windows Vista и более новых версий Windows. Также можно создать беспроводную политику для компьютеров под управлением Windows XP.

Если щелкнуть правой кнопкой мыши на узле Политики проводной сети (IEEE 802.3) (Wired Network), можно создать политику для Windows Vista и более поздних версий ОС, которая определяет, будет ли использоваться служба Wire AutoConfig для настройки и подключения этих клиентов к проводным 802.3 Ethernet-сетям. Для Windows 7 и более поздних версий Windows доступны опции, запрещающие использование общих учетных данных и включающие период блокировки, что запрещает компьютерам производить автподключение к сети на указанный период времени.

Если сетевое обнаружение не включается (нет никаких ошибок, просто при нажатии кнопки Сохранить изменения переключатель остается в положении Отключить сетевое обнаружение), убедитесь, что включены следующие службы: Обнаружение SSDP, Модуль поддержки NetBIOS через TCP/IP, Браузер компьютеров, Сервер и Публикация ресурсов обнаружения функции. Эти службы (или некоторые из них) по умолчанию могут быть выключены на Windows Server. Такова особенность серверной версии Windows

Если щелкнуть правой кнопкой мыши на узле Политики беспроводной сети (IEEE 802.11), у вас будет возможность создать разные политики — для компьютеров под управлением Windows XP и для компьютеров с более новыми версиями Windows. Данные поли тики включают автонастройку WLAN, определяют, какие сети могут быть использованы, и устанавливают сетевые разрешения. Для Windows 7 и более поздних версий есть возможность запрещения использования общих учетных данных, включения периода блокировки, а также запрещения размещенных сетей.

ОС Windows Vista SP1 и более поздние версии поддерживают несколько проводных и беспроводных расширений. Эти расширения позволяют пользователям изменять свои пароли при подключении к проводной или беспроводной сети (в противовес использованию функции изменения

пароля Winlogon), исправлять неправильный пароль, введенный во время входа и сброса истекшего пароля — все это часть процесса сетевого входа.
Расширения сетевой безопасности включают следующие протоколы:

- протокол SSTP (Secure Socket Tunneling Protocol);
- безопасный удаленный доступ SRA (Secure Remote Access);
- интерфейс CryptoAPI Version 2 (CAPI2);
- расширения протокола OCSP (Online Certificate Status Protocol);
- резервирование порта для протокола Teredo;
- подпись файла по протоколу RDP (Remote Desktop Protocol).

Протокол SSTP позволяет передавать данные на канальном уровне по протоколу HTTP через подключение HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer). Технология SPA обеспечивает безопасный доступ к удаленным сетям по HTTPS. Вместе обе технологии позволяют пользователям получать защищенный доступ к частной сети посредством интернет-соединения. Протоколы SSTP и SPA представляют собой модификации PPTP (Point-to-Point Tunneling Protocol) и L2TP/IPsec (Layer Two Tunneling Protocol/Internet Protocol). Для защищенного веб-трафика они используют стандартные порты TCP/IP, что позволяет им проходить через большинство брандмауэров, а также преобразование сетевых адресов NAT (Network Address Translation) и веб-прокси.
Протокол SSTP использует HTTP по протоколу SSL (HTTP over Secure Sockets Layer), который так же известен, как TLS (Transport Layer Security). Протокол HTTP по SSL (TCP-порт 443) обычно служит для защищенной связи с веб-сайтами. Каждый раз, когда пользователи подключаются к веб-адресу, который начинается с https://, они используют HTTP по SSL.
Использование HTTP по SSL решает множество проблем VPN-подключений. Поскольку SSTP поддерживает и IPv4, и IPv6, то пользователи могут установить безопасные соединения, используя любую версию IP. По сути, вы получите технологию VPN, которая работает всегда и везде.
Интерфейс CAPI расширяет поддержку сертификатов PKI и X.509, а также реализует дополнительную функциональность для проверки пути, хранилищ сертификатов и проверку подписи. Один из этапов проверки пути сертификата — это проверка аннулирования (отзыв), включающая в себя проверку состояния сертификата, чтобы убедиться, что он не был отозван издателем. Здесь на сцене появляется протокол онлайн-проверки состояния сертификата (Online Certificate Status Protocol, OCSP).

Протокол OCSP используется для проверки состояния аннулирования сертификатов. Также CAPI2 поддерживает независимые цепочки подписей OCSP и определяет дополнительные источники загрузки OCSP для каждого издателя. Независимые цепочки подписей OCSP изменяют исходную реализацию OCSP так, что он может работать с OCSP-откликами, подписанными доверенными источниками OCSP, которые не связаны с издателем проверяемого сертификата. Дополнительные источники загрузки OCSP позволяют указать источники загрузки OCSP для выпуска CA-сертификатов в виде URL, которые добавляются как свойства к CA-сертификатам.

Чтобы гарантировать сосуществование IPv4/IPv6, Windows позволяет приложениям использовать IPv6 в сети IPv4, и это позволяет использовать соответствующие технологии, например резервирование порта для Teredo. Teredo — технология туннелирования на базе протокола UDP (User Datagram Protocol), способная пройти через NAT. Она устанавливает связь между симметричными NAT с резервированием портов и прочими типами NAT. Механизм NAT с резервированием портов использует внешний порт с тем же номером, что и внутренний.

Текущие выпуски Windows Server поддерживают технологию разгрузки процессора TCP Chimney. Эта функция позволяет перенести обработку TCP/IP-соединения с процессоров сервера на его сетевые адаптеры, если они поддерживают функцию разгрузки TCP/IP. Могут быть разгружены как TCP/IPv4-соединения, так и TCP/IPv6. По умолчанию TCP-соединения разгружаются на Ethernet-адаптерах, работающих со скоростью 10 Гбит/с, но эта функция выключена на адаптерах со скоростью 1 Гбит/с. Для изменения соответствующих настроек можно использовать Netsh.

Инфраструктура диагностики сети (Network Diagnostic Framework, NDF) упрощает поиск неполадок путем автоматизации множества этапов поиска неисправности и предоставления готовых решений. При использовании утилиты Диагностика сети Windows (Windows Network Diagnostics) каждый сеанс диагностики генерирует отчет с ее результатами, а просмотреть эту информацию можно в Центре поддержки (Action Center), щелкнув по ссылке Устранение неполадок (Troubleshooting), а затем нажав кнопку Просмотр журнала (View History). На странице Журнал устранения неполадок (Troubleshooting History) каждый сеанс выводится по типу и дате запуска. Для просмотра подробной информации щелкните на сеансе, который нужно просмотреть, и нажмите кнопку Подробности (View details).

Диагностическая информация, показанная в Центре поддержки, приходит из файла ETL (Event Trace Log), создаваемого при диагностике. Если щелкнуть правой кнопкой мыши по сеансу диагностики, в контекстном меню будет команда Открыть расположение файла (Open File Location).

Выбрав ее, можно увидеть все сгенерированные файлы диагностики для выбранного сеанса диагностики.
Контекст Netsh Trace может быть использован для осуществления всесторонней трассиров-ки, а также захвата и фильтрации пакетов. Трассировки выполняются с использованием предопределенных или пользовательских сценариев и провайдеров. Сценарии трассировки — это коллекции провайдеров. Провайдеры — это фактические компоненты в стеке сетевого протокола, с которыми нужно работать, такие как TCP/IP, Платформа фильтрации Windows и брандмауэр, Службы беспроводной сети, Winsock или NDIS. Как правило, для анализа данных трассировки используется приложение Сетевой монитор (Network Monitor, Netmon). Если нужно собрать данные трассировки по компьютеру, где не установлен Сетевой монитор, можно просто скопировать файл трассировки на компьютер, где установлено это приложение, чтобы проанализировать данные.
В Windows Vista SP1 и более поздних версиях используется клиент RDP 6.1, который позволяет подписывать файлы RDP для предотвращения открытия или запуска пользователями потенциально опасных файлов из неизвестных источников. Администраторы могут подписывать файлы RDP при помощи специального инструментария Microsoft. В групповой политике или реестре могут быть настроены три связанных параметра: разделенный запятыми список хэшей сертификатов, которым доверяют администраторы (список доверенных издателей), параметр, позволяющий пользователям принимать недоверенных издателей (включен по умолчанию), а также параметр, позволяющий принимать неподписанные файлы (включен по умолчанию).

Установка сети TCP/IP

Для установки сети на компьютере нужно установить поддержку TCP/IP и сетевой адаптер. В системе Windows Server 2012 протокол TCP/IP используется в качестве стандартного протокола глобальных сетей. Обычно установка сети происходит одновременно с установкой Windows Server 2012. Администратор также может установить протокол TCP/IP в свойствах подключения по локальной сети.
Для установки TCP/IP после установки Windows Server 2012 зайдите в компьютер, используя учетную запись с привилегиями администратора, и выполните следующие действия:

1. В Панели управления откройте Центр управления сетями и общим доступом, щелкнув по ссылке Просмотр состояния сети и задач (View network status and tasks) под заголовком Сеть и Интернет (Network and Internet).
2. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера (Change adapter settings).

3. На странице Сетевые подключения (Network Connections) щелкните правой кнопкой мыши по соединению, параметры которого нужно изменить, выберите команду Свойства. Откроется окно свойств для подключения.
4. Если в списке отсутствуют Протокол Интернета версии 6 (TCP/IPv6) (Internet Protocol Version 6 (TCP/IPv6)) и Протокол Интернета версии 4 (TCP/IPv4) (Internet Protocol Version 4 (TCP/IPv4)), нужно установить их. Нажмите кнопку Установить (Install), а затем выберите элемент Протокол (Protocol) и нажмите кнопку Добавить (Add). В окне Выбор сетевого протокола (Select Network Protocol) выберите протокол для установки и затем нажмите кнопку OK. Если устанавливается и TCP/IPv6, и TCP/IPv4, повторите эту процедуру для каждого протокола.
5. В окне свойств для сетевого подключения убедитесь, что оба протокола (TCP/IPv6 и TCP/IPv4) выбраны, и нажмите кнопку OK.
6. При необходимости следуйте инструкциям следующего раздела для настройки сетевых подключений компьютера.

Настройка TCP/IP-сети

Подключение по локальной сети создается автоматически, если в компьютере есть сетевой адаптер и он подключен к сети. Если на компьютере установлено несколько сетевых адаптеров, у каждого из них будет собственное подключение к локальной сети. Если доступных сетевых подключений не существует, следует подключить компьютер к сети или создать подключение другого типа.
Для работы по протоколу TCP/IP компьютеру необходим IP-адрес. В Windows Server 2012 существует несколько способов настройки IP-адреса.

- Вручную. IP-адреса, назначаемые вручную, называются статическими IP-адресами. Такие фиксированные адреса не изменяются, пока администратор не изменит их. Как правило, статические IP-адреса назначаются серверам Windows. При этом следует настроить также ряд дополнительных параметров, чтобы помочь серверу "освоиться" в сети.
- Динамически. Динамические IP-адреса назначаются во время запуска компьютера DHCP-сервером (если он установлен в сети). Время от времени такие адреса могут изменяться. По умолчанию все IP-адреса компьютера считаются динамическими.
- Альтернативный адрес (только для IPv4). Когда компьютер настроен на использование DHCPv4, но в сети нет доступного DHCPv4-сервера, ОС Windows Server 2012 автоматически назначает компьютеру частный альтернативный IP-адрес. По умолчанию альтернативный адрес IPv4 назначается из диапазона 169.254.0.1—169.254.255.254 с маской подсети 255.255.0.0. Также

можно назначить пользовательский альтернативный IPv4- адрес, что особенно полезно на ноутбуке.

Настройка статического IP-адреса

При назначении статического IP-адреса кроме самого IP-адреса нужно указать маску подсети, а также, при необходимости, шлюз по умолчанию для межсетевого взаимодействия.

IP-адрес — это числовой идентификатор компьютера. Схемы IP-адресации различаются в зависимости от настройки сети, но в большинстве случаев они назначаются на основе конкретных сетевых сегментов.

Адреса IPv6 сильно отличаются от адресов IPv4. В IPv6-адресах первые 64 бита представляют идентификатор сети, а оставшиеся 64 бита — сетевой интерфейс. В IPv4-адресах переменное число первых битов обозначает идентификатор сети, а остальные биты — идентификатор хоста. Допустим, используется протокол IPv4 и компьютер в сегменте сети 10.0.10.0 с маской подсети 255.255.255.0. Первые три группы битов обозначают сетевой идентификатор, а доступные для хостов адреса находятся в диапазоне от 10.0.10.1 до 10.0.10.254. Адрес 10.0.10.255 зарезервирован для широковещательной передачи.

Если компьютер находится в частной сети, не имеющей прямого выхода в Интернет, следует использовать частные IPv4-адреса, приведенные в табл. 14.1.

Таблица 14.1. Частные сетевые IPv4-адреса

Идентификатор частной сети	Маска сети	Диапазон сетевых адресов
10.0.0.0	255.0.0.0	10.0.0.0— 10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0— 172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0— 192.168.255.255

Все остальные сетевые IPv4-адреса являются публичными и должны арендоваться или приобретаться. Если сеть подключена напрямую к Интернету, получите диапазон IPv4-адресов от интернет-провайдера и назначайте их компьютерам.

Использование команды ping для проверки IP-адреса

Прежде чем назначить статический IP-адрес, убедитесь, что он не занят и не зарезервирован для использования с DHCP. Проверить использование адреса можно при помощи команды *ping*. Откройте командную строку и введите *ping* с IP-адресом, который хотите проверить. Например, для проверки IPv4-адреса 10.0.10.12 нужно ввести команду:

ping 10.0.10.12

Команда для проверки IPv6-адреса FEC0::02BC:FF:BECB:FE4F:961D выглядит так:
ping FEC0::02BC:FF:BECB:FE4F:9610
Если команда *ping* даст положительный ответ, данный IP-адрес уже используется, и необходимо проверить другой адрес. Если время запроса всех четырех попыток команды *ping* истекло, а отклик от компьютера так и не получен, IP-адрес в настоящий момент не активен и, возможно, не используется. Однако запросы *ping* могут блокироваться брандмауэром.
Информацию об использовании адреса также может предоставить администратор сети компании.

Настройка статического IPv4- или IPv6-адреса

Каждый установленный сетевой адаптер может быть подключен к одной локальной сети. Подключения создаются автоматически. Для настройки IP-адреса конкретного подключения выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. На странице Сетевые подключения щелкните правой кнопкой мыши по соединению, с которым необходимо работать, выберите команду Свойства.
2. Дважды щелкните на протоколе TCP/IPv6 или TCP/IPv4 в зависимости от того, какой тип IP-адреса нужно настроить.
3. Для IPv6-адреса сделайте следующее.
   - Выберите переключатель Использовать следующий IPv6-адрес (Use the following IPv6 address) и затем введите IPv6-адрес в поле IPv6-адрес (IPv6 address). Введенный вами IPv6-адрес не должен использоваться на каком-либо другом компьютере сети.
   - Поле Длина префикса подсети (Subnet prefix length) обеспечивает нормальный доступ компьютера к сети. ОС Windows Server 2012 вставляет в поле Длина префикса подсети стандартное значение префикса. Если в сети не используются подсети переменной длины, стандартное значение должно сработать. В противном случае придется привести значение в соответствие с сетью.
4. Для IPv4-адреса сделайте следующее.
   - Выберите переключатель Использовать следующий IP-адрес (Use the following IP address) и введите IPv4-адрес в поле IP-адрес (IP address). Введенный IPv4-адрес должен быть уникален в пределах сети.
   - Поле Маска подсети (Subnet mask) обеспечивает нормальный доступ компьютера к сети. ОС Windows Server 2012 автоматически вставляет в поле значение маски по умолчанию. Если в сети не используются подсети

переменной длины, стандартное значение должно сработать. В противном случае придется привести значение в соответствие с сетью предприятия.

5. Если компьютеру необходим выход в другие TCP/IP-сети, в Интернет или другие подсети, укажите IP-адрес шлюза по умолчанию в поле Основной шлюз (Default gateway).

6. Доменная система имен (DNS) необходима для разрешения доменных имен. Введите адреса предпочитаемого и альтернативного DNS-серверов в предоставленные поля.

7. Когда закончите, нажмите кнопку OK дважды. Повторите этот процесс для других сетевых адаптеров и IP-протоколов, которые необходимо настроить.

8. При использовании IPv4-адресации настройте WINS при необходимости.

Настройка динамических и альтернативных IP-адресов

Хотя у большинства серверов есть статические IP-адреса, можно настроить серверы для использования динамических и альтернативных IP-адресов или их комбинаций. Для настройки динамической и альтернативной адресации выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. На странице Сетевые подключения для каждого установленного сетевого адаптера отображается одно подключение по локальной сети. Подключения создаются автоматически. Если для установленного адаптера сетевое подключение не отображается, проверьте драйвер адаптера. Возможно, он установлен неправильно.

Щелкните правой кнопкой мыши по нужному подключению и выберите команду Свойства.

2. Дважды щелкните на TCP/IPv6 или TCP/IPv4 в зависимости от типа настраиваемого IP-адреса.

3. Выберите переключатель Получить IPv6-адрес автоматически (Obtain an IPv6 address automatically) или Получить IP-адрес автоматически (Obtain an IP address automatically) в соответствии с типом настраиваемого IP-адреса. При необходимости установите также переключатель Получить адрес DNS-сервера автоматически (Obtain DNS server address automatically) или Использовать следующие адреса DNS-серверов (Use the following DNS server addresses), а затем введите адреса основного и альтернативного DNS-серверов в предоставленные поля.

4. При использовании динамического IPv4-адреса на настольном компьютере можно или использовать автоматический альтернативный адрес, или вручную настроить альтернативный

адрес. На вкладке Альтернативная конфигурация (Alternate Configuration) установите переключатель Автоматический частный IP-адрес (Automatic private IP address) для автоматического подключения альтернативного IP-адреса. Нажмите кнопку
OK, а затем кнопку Закрыть и пропустите оставшиеся действия.

5. Для задания альтернативного адреса вручную перейдите на вкладку Альтернативная конфигурация и выберите переключатель Настраиваемый пользователем (User configured), а затем введите IP-адрес, который планируется использовать. Указанный вами IP-адрес должен быть частным IP-адресом, т. е. принадлежать одному из диапазонов, и быть уникальным в пределах сети. Завершите альтернативную конфигурацию вводом маски сети, шлюза по умолчанию, DNS-сервера и WINS-сервера. Нажмите кнопку OK, а затем кнопку Закрыть.

Настройка нескольких шлюзов

Для обеспечения отказоустойчивости в случае отказа маршрутизатора можно настроить компьютеры на базе Windows Server 2012 так, что они будут использовать несколько основных шлюзов. При назначении нескольких шлюзов ОС Windows Server 2012 использует метрику шлюза для определения, какой шлюз задействовать и в какое время. Метрика шлюза характеризует затраты на маршрутизацию для данного шлюза. Первым используется шлюз с наименьшей метрикой. Если компьютер не может установить связь с этим шлюзом, ОС Windows Server 2012 пытается использовать шлюз, следующий по возрастанию метрики.

Выбор лучшего способа настройки нескольких шлюзов зависит от конфигурации сети. Если компьютеры в вашей организации настраиваются при помощи DHCP, вероятно, лучше задавать дополнительные шлюзы через параметры на DHCP-сервере. Если же компьютеры используют статические IP-адреса или нужно задавать IP-адреса шлюзов самостоятельно, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. На странице Сетевые подключения щелкните правой кнопкой мыши по необходимому соединению и выберите команду Свойства.

2. Дважды щелкните на TCP/IPv6 или TCP/IPv4 в зависимости от типа настраиваемого IP-адреса.

3. Нажмите кнопку Дополнительно (Advanced), чтобы открыть окно Дополнительные параметры TCP/IP (Advanced TCP/IP Settings).

4. Панель Основные шлюзы (Default gateways) показывает шлюзы, которые были настроены вручную (если таковые имеются). При необходимости введите адреса дополнительных шлюзов:

- нажмите кнопку Добавить и введите адрес шлюза в поле Шлюз (Gateway);
- по умолчанию Windows Server 2012 назначает метрику шлюзу автоматически, но можно задать ее вручную. Сбросьте флажок Автоматическое назначение метрики (Automatic metric) и введите метрику в соответствующее поле. Нажмите кнопку Добавить;
- повторите приведенные ранее действия для каждого шлюза, который необходимо добавить.

5. Нажмите кнопку OK, а затем кнопку Закрыть.

Настройка сети для Hyper-V

После установки Hyper-V и создания внешней виртуальной сети ваш сервер будет использовать виртуальный сетевой адаптер для подключения к физической сети. Страница Сетевые подключения покажет название исходного сетевого адаптера и новый виртуальный сетевой адаптер. К исходному сетевому адаптеру будет добавлен протокол Расширяемый виртуальный коммутатор Hyper-V (Microsoft Virtual Network Switch Protocol). У виртуального сетевого адаптера будут все стандартные протоколы и службы. Имя виртуального сетевого адаптера, отображающееся на странице Сетевые подключения, будет таким же, как и имя виртуального сетевого коммутатора, связанного с ним.

Для настройки Hyper-V можно создать внутреннюю виртуальную сеть, что позволит обмениваться данными только между сервером и размещенными виртуальными машинами.

В этом случае не будет необходимости связывать физический сетевой адаптер с виртуальным сетевым адаптером. Hyper-V связывает виртуальную сетевую службу с физическим адаптером, только когда создается внешняя сеть.

После установки Hyper-V на сервер и включения внешней виртуальной сети будет использоваться переключение виртуальной сети.

У сервера есть сетевое подключение с включенным протоколом Расширяемый виртуальный коммутатор Hyper-V (Hyper-V Extensible Virtual Switch Protocol), все остальные компоненты сетевого адаптера выключены. Для виртуального сетевого адаптера основные сетевые компоненты включены, а протокол Расширяемый виртуальный коммутатор Hyper-V выключен. Такая конфигурация необходима для корректной коммуникации между сервером и виртуальными машинами. Если эту конфигурацию изменить, виртуальные машины не смогут подключаться к внешней сети.

Управление сетевыми подключениями

Сетевые подключения позволяют компьютерам получать доступ к ресурсам в сети и в Интернете. Для каждого установленного на компьютере сетевого адаптера автоматически устанавливается одно подключение по локальной сети. В этом разделе рассмотрены способы управления подключениями.

Проверка состояния, скорости и активности сетевого подключения

Для проверки состояния сетевого соединения выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. На странице Сетевые подключения щелкните правой кнопкой мыши по соединению и выберите команду Состояние (Status).
2. Будет открыто окно Состояние (Status) для сетевого подключения. Если подключение выключено или кабель не подключен, это окно не откроется. Включите подключение или подключите сетевой кабель для решения проблемы, а затем снова попытайтесь отобразить окно Состояние.

Включение или отключение сетевых подключений

Сетевые подключения создаются и подключаются автоматически. Если нужно отключить соединение так, чтобы его нельзя было использовать, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. На странице Сетевые подключения щелкните правой кнопкой мыши по соединению, которое нужно отключить, выберите команду Отключить (Disable) для отключения соединения.
2. Если необходимо включить подключение позже, щелкните правой кнопкой мыши на подключении и выберите команду Включить (Enable).

Если необходимо отключиться от сети, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. На странице Сетевые подключения щелкните правой кнопкой мыши по соединению и выберите команду Отключить.
2. Если позже понадобится активировать подключение, щелкните по нему правой кнопкой мыши и выберите команду Подключить (Connect).

Переименование сетевых подключений Операционная система Windows Server 2012 автоматически назначает имена сетевым

подключениям. На странице Сетевые подключения можно переименовать подключение, щелкнув по нему правой кнопкой мыши и выбрав команду Переименовать (Rename).

После этого нужно ввести новое имя. Если у компьютера много сетевых подключений, используйте информативные имена, чтобы понимать назначение каждого соединения.

ГЛАВА 2 Запуск DCHP-клиентов и серверов

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) используется для упрощения администрирования доменов Active Directory, и в этой главе будет рассказано, как это сделать. Протокол DHCP служит для динамического назначения конфигурационной информации TCP/IP-клиентам сети. Протокол не только экономит время, необходимое на настройку клиентов сети, но и предоставляет централизованный механизм для обновления конфигурации. Для включения DHCP в сети нужно установить и настроить DHCP-сервер. Этот сервер отвечает за назначение необходимой сетевой информации.

Обзор DHCP

Протокол DHCP предоставляет централизованное управление IP-адресацией и многое другое. После установки DHCP с его помощью можно передавать клиентам сети всю необходимую для настройки TCP/IP информацию, а именно: IP-адрес, маску сети, основной шлюз, адреса основного и альтернативного DNS-серверов, адреса основного и альтернативного WINS-серверов, доменное имя компьютера. DHCP-серверы могут назначать динамические адреса IPv4 и/или IPv6 любой сетевой карте (Network Interface Card, NIC) компьютера.

Динамическая IPv4-адресация

Компьютер, использующий динамическую адресацию и настройку параметров протокола IPv4, называется DHCPv4-клиентом. При загрузке DHCPv4-клиента из пула IPv4-адресов, выделенного DHCP-серверу, извлекается 32-разрядный IPv4-адрес и назначается клиенту на определенный период времени, называемый сроком аренды. По истечении примерно половины срока аренды клиент пытается ее продлить. Если попытка не удалась, до истечения срока аренды клиент ее повторит. В случае неудачи клиент попытается связаться с другим DHCP-сервером. IPv4-адреса, аренда которых не продлена, возвращаются в пул адресов. Если клиенту удается связаться с сервером DHCP, но нет возможности продлить аренду текущего IP-адреса, DHCP-сервер назначает клиенту новый IPv4-адрес.

Доступность DHCP-сервера не влияет на запуск или вход в систему (в большинстве случаев). Даже если DHCP-сервер недоступен, DHCPv4-

клиенты могут быть запущены и пользователи могут войти в локальный компьютер. Во время запуска клиент DHCPv4 производит поиск DHCP-сервера. Если DHCP-сервер доступен, клиент получает у него информацию о настройках. Если DHCP-сервер недоступен, но срок аренды еще не истек, клиент "пингует" основной шлюз, записанный в параметрах аренды. Успех операции свидетельствует, что клиент находится в той же сети, в которой он был на момент предоставления аренды. Клиент продолжает пользоваться арендой, как было описано ранее. Неудача команды *ping* говорит о том, что клиент находится в другой сети. В этом случае клиент использует автоматическую настройку IPv4. Она также применяется, если DHCP-сервер не доступен, а срок предыдущей аренды истек.

Автоматическая настройка IPv4 работает следующим образом:

1. Клиентский компьютер выбирает IP-адрес из подсети класса B 169.254.0.0 с маской подсети 255.255.0.0, зарезервированной Microsoft. Перед использованием IPv4-адреса клиент при помощи протокола ARP проверяет, что данный IPv-адрес не занят другим клиентом.
2. Если адрес занят, клиент повторяет шаг 1. После десяти неудачных попыток произойдет ошибка. Если клиент отключен от сети, результат ARP-тестирования всегда будет успешным, поэтому клиент получит первый попавшийся IPv4-адрес.
3. Если выбранный IPv4-адрес доступен, клиент соответствующим образом настраивает сетевой адаптер. Далее, клиент пытается связаться с DHCP-сервером, каждые пять минут посылая в сеть запрос. После успешной установки связи клиента с сервером клиент получает аренду и заново настраивает сетевой интерфейс.

Администратор должен определить, сколько DHCP-серверов нужно установить в сети. Обычно нужно как минимум два DHCP-сервера в физическом сегменте сети. Операционная система Windows Server 2012 поддерживает отказоустойчивость DHCP для IPv4. Отказоустойчивость предполагает высокую доступность DHCP-сервисов путем синхронизации информации об аренде IPv4-адресов между двумя DHCP-серверами в одном из двух режимов.

- Режим балансировки нагрузки (Load Balance). В этом режиме администратор указывает процентное соотношение загрузки каждого сервера. Обычно используется соотношение 50/50, чтобы нагрузка на каждый сервер была одинаковой. Но можно использовать другие соотношения, например 60/40, при этом один сервер будет обрабатывать 60% запросов, другой — 40%.
- Режим горячего резервирования (Hot Standby). В этом режиме один из серверов действует как основной сервер и обрабатывает DHCP-запросы. Другой сервер является резервным и используется, когда произошел сбой основного сервера или на основном сервере

закончились IP-адреса для аренды. Обычно для резервного сервера резервируется 5% IP-адресов.

Настройка отказоустойчивости DHCP предельно проста и не требует кластеризации или какой-либо другой расширенной настройки. Для настройки отказоустойчивости DHCP нужно выполнить следующие действия:

1. Установите и настройте два DHCP-сервера. Серверы должны находиться в одной и той же физической сети.
2. Создайте область DHCPv4 на одном из серверов. Область — это пул IPv4- или IPv6- адресов, которые можно назначить клиентам с помощью аренды.
3. Как только укажете, что другой сервер является партнером отказоустойчивости для области DHCPv4, область будет реплицирована партнеру.

Динамическая IPv6-адресация

Если в процессе установки системы на компьютере обнаружено сетевое оборудование, по умолчанию включаются оба протокола (IPv4 и IPv6). Как было сказано в главах 1 и 14, IPv4 — основная версия протокола IP, используемая в большинстве сетей, а IPv6 — это следующая версия протокола IP. В протоколе IPv6 используются 128-разрядные адреса.

В стандартной конфигурации первые 64 бита — это идентификатор сети, а последние 64 бита — сетевой интерфейс на клиентском компьютере.

Существуют два режима настройки IPv6-адресации средствами DHCP.

1. Режим с отслеживанием состояния (DHCPv6 stateful mode). В этом режиме DHCPv6-клиенты получают IPv6-адреса и параметры настройки сети от DHCPv6-сервера.
2. Режим без отслеживания состояния (DHCPv6 stateless mode). В этом режиме DHCPv6-клиенты получают IP-адреса при помощи автоматической настройки, а параметры сетевой конфигурации — при помощи DHCPv6.

Компьютер, получающий от DHCPv6-сервера IPv6-адрес и/или сетевые настройки, называется DHCPv6-клиентом. Как и в случае DHCPv4, инфраструктура DHCPv6 состоит из DHCPv6-клиентов, запрашивающих параметры, DHCPv6-серверов, предоставляющих параметры, и агентов-ретрансляторов DHCPv6, которые обеспечивают обмен данными между клиентами и серверами, когда клиенты находятся в подсетях, не имеющих DHCPv6-сервера.

В отличие от DHCPv4, для поддержки DHCPv6 придется настроить IPv6-маршрутизаторы. В основе автоматической настройки DHCPv6 лежат следующие флаги в сообщении, посылаемом ближайшим маршрутизатором:

- флаг Managed Address Configuration (флаг M) — если этот флаг установлен в 1, он предписывает клиенту использовать протокол для получения адресов с отслеживанием состояния;
- флаг Other Stateful Configuration (флаг O) — если этот флаг установлен в 1, он предписывает клиенту использовать протокол для получений других параметров.

Клиент DHCPv6 имеется в любой современной версии Windows (начиная с Vista). Он выстраивает конфигурацию DHCPv6 в зависимости от значений флагов M и O в полученных им объявлениях маршрутизатора. Если в данной сети несколько объявляющих маршрутизаторов, их следует настроить так, чтобы для флагов M и O объявлялись одинаковые значения и префиксы адреса без отслеживания состояния. У клиентов IPv6 под управлением Windows XP или Windows Server 2003 нет DHCPv6-клиента, поэтому они игнорируют флаги M и O в объявлениях маршрутизаторов.

Можно настроить маршрутизатор IPv6 на установку в объявлениях значения 1 для флага M. Для этого в командной строке с повышенными полномочиями нужно ввести команду:

netsh interface ipv6 set interface InterfaceName managedaddress=enabled

Здесь InterfaceName — фактическое имя интерфейса.

Аналогичным способом можно установить значение 1 для флага O в объявлениях, введя в командной строке с повышенными полномочиями команду:

netsh interface ipv6 set interface InterfaceName otherstateful=enabled

Если в имени интерфейса присутствуют пробелы, его следует заключить в кавычки, как в следующем примере:

netsh interface ipv6 set interface "Wired Ethernet Connection 2" managedaddress=enabled

Работая с флагами M и O, помните о следующем.

- Если оба флага имеют значение 0, считается, что в сети нет инфраструктуры DHCPv6. Клиенты используют объявления маршрутизатора для настройки нелокальных адресов и ручную настройку других параметров.
- Если оба флага имеют значение 1, DHCPv6 используется для назначения как IP-адресов, так и других параметров конфигурации. Эта комбинация известна как режим с отслеживанием состояния, при котором DHCPv6 назначает IPv6-клиентам адреса.
- Если значение флага M равно 0, а значение флага O — 1, DHCPv6 используется только для назначения прочих параметров конфигурации. Соседние маршрутизаторы настроены на объявление префиксов нелокальных адресов, из которых клиенты IPv6 получают адреса без отслеживания состояния. Эта комбинация известна как режим без отслеживания состояния.

– Если значение флага M равно 1, а значение флага O — 0, DHCPv6 используется для настройки IP-адресов, но не других параметров. Поскольку IPv6-адреса следует, как правило, настраивать вместе с другими параметрами, например IPv6-адресами DNS-серверов, данная комбинация применяется редко.

ОС Windows получает динамические IPv6-адреса примерно так же, как и адреса IPv4. Обычно автоматическая настройка IPv6 для клиентов DHCPv6 в режиме с отслеживанием состояния происходит так:

1. Клиентский компьютер получает индивидуальный локальный IPv6-адрес с отслеживанием состояния. Перед использованием IPv6-адреса клиент при помощи ARP проверяет, что данный IPv6-адрес не используется другим клиентом.
2. Если адрес занят, клиент повторяет шаг 1. Помните, что если клиент отключен от сети, результат ARP-тестирования всегда успешный. Поэтому клиент получает первый попавшийся IPv6-адрес.
3. Если выбранный IPv6-адрес доступен, клиент соответствующим образом настраивает сетевой адаптер. Далее клиент пытается связаться с DHCP-сервером, каждые пять минут посылая запрос в сеть. После успешной установки связи клиента с сервером клиент получает аренду и заново настраивает сетевой интерфейс.

Иначе работает автоматическая настройка параметров IPv6 на клиентах DHCPv6 в режиме без отслеживания состояния. В этом случае клиенты DHCPv6 настраивают как локальные адреса, так и дополнительные нелокальные адреса, обмениваясь запросами и объявлениями с соседними маршрутизаторами.

Как и в случае DHCPv4, в протоколе DHCPv6 используются сообщения UDP. Клиенты DHCPv6 принимают сообщения на UDP-порт 546. Серверы и агенты-ретрансляторы DHCPv6 принимают сообщения на UDP-порт 547. Структура сообщений DHCPv6 намного проще, чем структура сообщений DHCPv4 — наследника протокола BOOTP, который служит для поддержки бездисковых рабочих станций.

Сообщения DHCPv6 начинаются с 1-байтового поля Msg-Type (тип сообщения). За ним следует 3-байтовое поле Transaction-ID, определяемое клиентом и служащее для группирования сообщений DHCPv6. За полем Transaction-ID следуют параметры DHCPv6 — идентификаторы сервера и клиента, адреса и прочие параметры.

С каждым параметром DHCPv6 связаны три поля. Поле Option-Code (2 байта) идентифицирует параметр. Поле Option-Len (2 байта) указывает на длину поля Option-Data в байтах. Поле Option-Data содержит данные соответствующего параметра.

У сообщений, пересылаемых между агентами-ретрансляторами и серверами, иная структура. Поле Hop-Count (1 байт) указывает на

количество агентов-ретрансляторов, получивших сообщение. Агент, получивший сообщение, может отбросить его, если значение счетчика переходов превысило заданный предел. Поле Link-Address длиной 15 байт содержит нелокальный адрес интерфейса, подключенного к подсети, в которой расположен клиент. На основе информации из поля Link-Address сервер устанавливает корректный диапазон, из которого следует извлекать адрес. Поле Peer-Address длиной 15 байт содержит IPv6-адрес клиента, пославшего сообщение, или агента, ретранслировавшего это сообщение. За полем Peer-Address следуют параметры DHCPv6. Основной параметр Relay Message обеспечивает инкапсуляцию сообщений, передаваемых между клиентом и сервером.

У протокола IPv6 нет широковещательных адресов. Вместо них в DHCPv6 пришел адрес All_DHCP_Relay_Agents_and_Servers, значение которого равно FF02::1:2. Чтобы обнаружить расположение DHCPv6-сервера в сети, клиент DHCPv6 отправляет Solicit-запрос со своего локального адреса. Если в подсети клиента есть DHCPv6-сервер, он получает Solicit-запрос и отправляет соответствующий ответ. Если клиент и сервер находятся в различных подсетях, агент-ретранслятор DHCPv6 в подсети клиента, который получает Solicit-запрос, перешлет его на DHCPv6-сервер.

Проверка назначения IP-адреса

Утилиту *Ipconfig* можно использовать для проверки назначенного в данный момент IP-адреса и другой конфигурационной информации. Чтобы получить информацию обо всех сетевых адаптерах компьютера, введите команду ipconfig /all. Если IP-адрес был назначен автоматически, будет выведено поле IP-адрес автонастройки (Autoconfiguration IP Address). В следующем примере автоматически настроен адрес 169.254.98.59:

```
Настройка протокола IP для Windows
Имя компьютера .............: DELTA
Основной DNS-суффикс.........: microsoft.com
Тип узла ...................: Смешанный
IP-маршрутизация включена ...: Нет
WINS-прокси включен . . . ...: Нет
Список поиска суффиксов DNS..: microsoft.com
Ethernet adapter Ethernet:
DNS-суффикс подключения .....:
Описание ....................: Intel Pro/1000 Network Connection
Физический адрес.............: 23-15-C6-F8-FD-67
DHCP включен.................: Да
Автонастройка включена.......: Да
IP-адрес автонастройки.......: 169.254.98.59
Маска подсети ..............: 255.255.0.0
Основной шлюз ..............:
```

DNS-серверы .....:

Области адресов

Области адресов — это пулы, диапазоны IPv4- и IPv6-адресов, которые могут арендовать клиенты.

Протокол DHCP также позволяет предоставлять адреса в бессрочную аренду. Чтобы зарезервировать конкретный IPv4-адрес, свяжите его с MAC-адресом компьютера, которому должен назначаться этот IPv4-адрес. В результате клиентский компьютер с указанным MAC-адресом будет всегда получать заданный IPv4-адрес. В протоколе IPv6 резервирование осуществляется посредством указания бессрочной аренды.

Администратором создаются области для определения диапазонов IP-адресов, доступных DHCP-клиентам. Например, можно назначить диапазон IP-адресов от 192.168.12.2 до 192.168.12.250 для области Предприятие. В областях допускается использование открытых или частных IPv4-адресов в следующих сетях:

сети класса A — IP-адреса в диапазоне от 1.0.0.0 до 126.255.255.255;
сети класса B — IP-адреса в диапазоне от 128.0.0.0 до 191.255.255.255;
сети класса C — IP-адреса в диапазоне от 192.0.0.0 до 223.255.255.255;
сети класса D — IP-адреса в диапазоне от 224.0.0.0 до 239.255.255.255.

IP-адрес 127.0.01 используется для локальной петли (loopback). В областях можно также использовать локальные одноадресные IPv6-адреса, глобальные одноадресные и многоадресные IPv6-адреса. Локальные одноадресные адреса начинаются с FE80. Многоадресные адреса начинаются с FF00. Глобальные (в пределах сайта) индивидуальные адреса включают все остальные адреса, кроме :: (unspecified) и ::1 (loopback). Один DHCP-сервер может управлять несколькими областями. Для IPv4-адресов доступны четыре типа областей:

- обычные области — используются для назначения адресов в сетях классов A, B и C;
- многоадресные области — используются для назначения IP-адресов в сетях IPv4 класса D. Многоадресные IP-адреса применяются в качестве второстепенных, в дополнение к стандартным IP-адресам;
- суперобласти — это контейнеры для других областей, которые упрощают управление несколькими областями;
- области отказоустойчивости — области между двумя DHCP-серверами для повышения отказоустойчивости, предоставления избыточности и включения балансировки нагрузки.

В IPv6 доступны только обычные области. Хотя можно создавать области, охватывающие несколько сегментов сети, обычно эти сегменты принадлежат к одному классу сети, например, к классу C.

Необходимо настроить DHCPv4- и DHCPv6-ретрансляцию для ретрансляции широковещательных DHCPv4- и DHCPv6-запросов между

сетевыми сегментами. Настроить агенты ретрансляции можно с помощью протокола RRAS (Routing and Remote Access Service) и агента DHCP-ретрансляции (DHCP Relay Agent Service). Также можно настроить некоторые маршрутизации как агенты ретрансляции.

Установка DHCP-сервера

Динамическая IP-адресация возможна, только если в сети установлен DHCP-сервер. Используя мастер добавления ролей и компонентов (Add Roles and Features Wizard), администратор может установить DHCP-сервер в качестве службы роли, задать ее начальные настройки и авторизовать сервер в Active Directory. Предоставлять клиентам динамические IP-адреса могут только авторизованные DHCP-серверы.

Установка компонентов DHCP

Чтобы сервер под управлением ОС Windows Server 2012 функционировал как DHCP-сервер, выполните следующие действия:

1. Серверу DHCP должны быть назначены статические IPv4- или IPv6-адреса в каждой обслуживаемой ими подсети. Убедитесь, что у сервера есть статические IPv4- или IPv6-адреса.
2. В диспетчере серверов выберите команду меню Управление | Добавить роли и компоненты или щелкните по ссылке Добавить роли и компоненты (Add Roles and Features) на панели приветствия. Будет запущен мастер добавления ролей и компонентов. Если мастер отобразит страницу Перед началом работы, прочитайте приветствие и нажмите кнопку Далее.
3. На странице Выбор типа установки по умолчанию отмечен переключатель Установка ролей или компонентов. Нажмите кнопку Далее.
4. На странице Выбор целевого сервера можно выбрать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите либо сервер из пула серверов, либо сервер, на котором можно смонтировать виртуальный жесткий диск (VHD). Если добавляете роли и компоненты на VHD, нажмите кнопку Обзор, а затем используйте окно Обзор виртуальных жестких дисков для выбора VHD. Как только будете готовы продолжить, нажмите кнопку Далее.

   В списке серверов будут только серверы под управлением Windows Server 2012 и те, которые были добавлены в диспетчере серверов.
5. На странице Выбор ролей сервера выберите роль DHCP-сервер (DHCP Server). Если нужно установить дополнительные компоненты, от которых зависит устанавливаемый компонент, вы увидите соответствующее диалоговое окно. Нажмите кнопку

Добавить компоненты для закрытия этого окна и установки требуемых компонентов на сервер.
Как только будете готовы продолжить, нажмите кнопку Далее.
6. Если на сервере, на который устанавливается роль DHCP-сервер, нет необходимых двоичных исходных файлов, сервер получит файлы через службу Windows Update (по умолчанию) или из расположения, указанного в групповой политике.
Также можно указать альтернативный источник для исходных файлов. Для этого щелкните по ссылке Указать альтернативный исходный путь (Specify An Alternate Source Path), в появившемся окне задайте альтернативный путь и нажмите кнопку OK. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer2012\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2-12\install.wim:4.
7. После просмотра опций установки сохраните их при необходимости, нажмите кнопку Установить для начала процесса установки. Страница Ход установки позволяет отслеживать процесс инсталляции. Если мастер был закрыт, нажмите значок Уведомления (Notifications) в диспетчере серверов, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.
8. Когда мастер закончит установку выбранных ролей и компонентов, страница Ход установки сообщит об этом. Просмотрите подробности установки и убедитесь, что все фазы инсталляции завершены успешно.
9. Для завершения установки DHCP-сервера нужна дополнительная конфигурация. Щелкните по ссылке Завершение настройки DHCP (Complete DHCP Configuration). Будет запущен мастер настройки DHCP после установки (DHCP Post-Install Configuration Wizard).
10. Панель Описание (Description) говорит о том, что для делегирования DHCP-сервера будут созданы группы Администратор DHCP (DHCP Administrators) и Пользователи DHCP (DHCP Users). Дополнительно, если DHCP-сервер присоединен к домену, его нужно авторизовать в Active Directory. Нажмите кнопку Далее.
11. На странице Авторизация (Authorization) укажите учетные данные, которые будут использоваться для авторизации этого DHCP-сервера доменными службами Active Directory.

- Текущее имя пользователя отображено в поле Имя пользователя (User name). Если у вас имеются привилегии администратора в домене, к которому присоединен DHCP-сервер, и нужно использовать текущие учетные данные, нажмите кнопку Фиксировать (Commit) для авторизации сервера с использованием этих учетных данных.

- Если нужно использовать альтернативные учетные данные или нельзя авторизовать сервер с использованием текущих учетных данных, установите флажок Использовать другие учетные данные (Use alternate credentials), а затем нажмите кнопку Указать (Specify). В окне Безопасность Windows (Windows Security) введите имя пользователя и пароль для авторизированной учетной записи и нажмите кнопку OK. Нажмите кнопку Фиксировать для попытки авторизации сервера с использованием этих учетных данных.
- Если нужно авторизовать DHCP-сервер позже, установите флажок Пропустить авторизацию AD (Skip AD Authorization) и нажмите кнопку Фиксировать. Помните, что в домене только авторизованные DHCP-серверы могут предоставлять клиентам динамические IP-адреса.

12. Когда мастер закончит постинсталляционную настройку, просмотрите сводку, убедитесь, что все задачи были выполнены успешно, и нажмите кнопку Закрыть.
13. Далее нужно перезагрузить службу DHCP-сервер на сервере, чтобы группы Администраторы DHCP и Пользователи DHCP могли использоваться. Для этого на левой панели консоли Диспетчер серверов выберите узел DHCP. Далее на главной панели, на панели СЕРВЕРЫ, выберите DHCP-сервер. На панели СЛУЖБЫ щелкните правой кнопкой мыши на службе DHCP-сервер и выберите команду Перезапустить службы (Restart service).
14. Для завершения инсталляции нужно сделать следующее.
    - Если у сервера есть несколько сетевых карт, пересмотрите привязку сервера и укажите соединения, которые DHCP-сервер будет использовать для обслуживания клиентов (см. разд. "Настройка привязок сервера" далее в этой главе).
    - Настройте параметры, которые будут передаваться DHCPv4- и DHCPv6-клиентам, в том числе 003 Router, 006 DNS Servers, 015 DNS Domain Name и 044 WINS/NBNS Servers (см. разд. "Установка параметров области" далее в этой главе).
    - Создайте и активируйте любые DHCP-области, которые будет использовать сервер (см. разд. "Создание областей и управление ими" далее в этой главе).

Запуск и использование консоли DHCP

После установки DHCP-сервера нужно использовать консоль DHCP для настройки и управления динамической IP-адресацией. В диспетчере серверов в меню Средства выберите команду DHCP. Основное окно консоли DHCP показано на рис. 15.1. Главное окно разделено на три

панели. Левая панель содержит список DHCP-серверов в домене (выводятся полные доменные имена серверов). Можно развернуть сервер, чтобы увидеть подузлы IPv4 и IPv6. Если развернуть IP-узлы, будут видны области и параметры, определенные для соответствующей версии IP. Центральная панель показывает расширенное представление выбранного элемента. Правая панель — панель действий, на ней представлены действия, которые можно выполнить над выделенными объектами. для создания и управления конфигурациями DHCP-сервера

Пиктограммы показывают текущее состояние узлов. Для серверов и IP-узлов можно увидеть следующие значки:

- галочка внутри зеленого кружочка указывает, что служба DHCP запущена и сервер активен;
- крестик в красном кружочке указывает, что консоль не может подключиться к серверу. Служба DHCP остановлена или сервер недоступен;
- красная стрелка вниз указывает, что DHCP-сервер не был авторизован;
- синий значок предупреждения указывает, что состояние сервера изменилось.

Для областей можно увидеть такие значки:

- красная стрелка вниз говорит о том, что область не была активирована;
- синий значок предупреждения указывает, что состояние области изменилось.

Подключение к удаленным DHCP-серверам

При запуске консоли DHCP она подключится к локальному DHCP-серверу, но в ней не будет записей удаленных DHCP-серверов. Подключиться к удаленным серверам можно с помощью следующих действий:

1. Щелкните правой кнопкой мыши на узле DHCP в дереве консоли и выберите команду Добавить сервер (Add Server). Откроется окно
2. Выберите переключатель Этот сервер (This server), а затем введите IP-адрес или имя компьютера DHCP-сервера, к которому нужно подключиться.
3. Нажмите кнопку OK. Запись для DHCP-сервера будет добавлена в дерево консоли.

Запуск и остановка DHCP-сервера

Управление DHCP-серверами осуществляется при помощи службы DHCP-сервер (DHCP Server). Как и любую другую службу, ее можно запустить, остановить, приостановить и перезапустить в узле Службы оснастки Управления компьютером или из командной строки. Кроме того, службой

DHCP-сервер можно управлять в консоли DHCP. Щелкните правой кнопкой мыши на сервере, которым хотите управлять, разверните подменю Все задачи (All Tasks) и выберите нужную команду: Запустить (Start), Остановить (Stop), Приостановить (Pause), Продолжить (Resume) или Перезапустить (Restart).
Можно также использовать консоль Диспетчер серверов для запуска и останова DHCP-сервера. Выберите DHCP на панели слева, далее на панели СЕРВЕРЫ выберите DHCP-сервер. Затем на панели СЛУЖБЫ щелкните правой кнопкой мыши по записи DHCP-сервер и выберите команду Запустить службы (Start Service), Остановить службы (Stop Service), Приостановить службы (Pause Service), Возобновить работу служб (Resume Service) или Перезапустить службы (Restart Service).

Авторизация DHCP-сервера в Active Directory

Прежде чем использовать DHCP-сервер в домене, его необходимо авторизовать в Active Directory. Авторизация сервера означает, что серверу разрешено назначать динамические IP-адреса в домене. В Windows Server 2012 авторизация требуется для предотвращения обслуживания клиентов неавторизованными DHCP-серверами.
Чтобы авторизовать DHCP-сервер, щелкните правой кнопкой мыши по элементу сервера в дереве консоли DHCP и выберите команду Авторизовать (Authorize). Чтобы лишить сервер авторизации, щелкните на нем правой кнопкой мыши и выберите команду Запретить (Unauthorize).

Настройка DHCP-серверов

После установки нового DHCP-сервера необходимо его настроить и оптимизировать для сетевого окружения. Для IPv4 и IPv6 предоставляются разные настройки.

Настройка привязок сервера

На сервере с несколькими сетевыми адаптерами имеется несколько подключений по локальной сети, по каждому из которых он может предоставлять параметры DHCP. Иногда работа DHCP на всех доступных подключениях не требуется. Допустим, на сервере имеются два подключения — 100 Мбит/с и 1 Гбит/с, и нужно пропускать трафик DHCP через подключение со скоростью 1 Гбит/с.
Чтобы связать DHCP с конкретным подключением, выполните следующие действия:

1. В консоли DHCP разверните узел сервера, с которым хотите работать. Щелкните правой кнопкой мыши на узле IPv4 или IPv6 и выберите команду Свойства.

2. В диалоговом окне свойств IPv4 или IPv6 перейдите на вкладку Дополнительно (Advanced) и нажмите кнопку Привязки (Add/Remove Bindings).
3. В диалоговом окне Привязки (Bindings) отображен список доступных сетевых подключений DHCP-сервера. Чтобы DHCP-сервер использовал подключение, установите соответствующий флажок. Чтобы подключение не использовалось, сбросьте соответствующий флажок.
4. Два раза нажмите кнопку OK, когда закончите.

Обновление DHCP-статистики

В консоли DHCP представлена статистика доступности и использования адресов IPv4 и IPv6. В консоли DHCP можно просмотреть эту статистику, развернув узел сервера, с которым нужно работать. Для этого щелкните правой кнопкой мыши на узле IPv4 или IPv6 (в зависимости от того, статистику по какому протоколу нужно просмотреть) и выберите команду Отобразить статистику (Display Statistics).
По умолчанию обновление статистики происходит только при запуске консоли DHCP, а также если выбрать сервер и нажать кнопку Обновление на панели инструментов. Если нет желания постоянно следить за DHCP, потребуется автоматическое обновление статистики. Для его настройки выполните следующие действия:

1. В консоли DHCP разверните узел сервера и щелкните правой кнопкой мыши на узле IPv4 или IPv6 и выберите команду Свойства.
2. На вкладке Общие установите флажок Автоматически обновлять статистику каждые (Automatically Update Statistics Every) и введите интервал обновления в часах и минутах. Нажмите кнопку OK.

Аудит и устранение неисправностей DHCP

По умолчанию Windows Server 2012 настроен на аудит процессов DHCP. Аудит отслеживает процессы и запросы DHCP и ведет журналы аудита.
Журналы аудита помогут в устранении неисправностей DHCP-сервера. По умолчанию оба протокола — IPv4 и IPv6 — производят запись в одни и те же журналы, но можно настроить и раздельный аудит. Стандартное расположение журналов DHCP — %SystemRoot%\ System32\DHCP. В этой папке находятся журналы для каждого дня недели. Файл журнала понедельника называется DhcpSrvLog-Mon.log, файл журнала вторника — Dhcp-SrvLog-Tue.log, и т. д.
При запуске DHCP-сервера или наступлении нового дня в файл журнала записывается заголовок. В заголовке содержится сводка событий DHCP и значение событий. При остановке и запуске службы DHCP-сервер очистка файла журнала может не произойти. Она обязательно выполняется по прошествии 24 часов с момента последней записи в журнал. Не нужно

отслеживать использование дискового пространства службой DHCP-сервер. Она по умолчанию настроена на ограничение используемого пространства. Включить или отключить аудит DHCP можно с помощью следующих действий:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, щелкните правой кнопкой мыши на узле IPv4 или IPv6 и выберите команду Свойства.
2. На вкладке Общие установите флажок Вести журнал аудита DHCP (Enable DHCP audit logging), а затем нажмите кнопку OK. По умолчанию журналы DHCP хранятся в папке %SystemRoot%\System32\DHCP. Можно изменить расположение журналов, выполнив следующие действия:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, щелкните правой кнопкой мыши на узле IPv4 или IPv6 и выберите команду Свойства.
2. Перейдите на вкладку Дополнительно. Поле Журнал аудита (Audit log file path) показывает текущее расположение журналов аудита. Введите имя новой папки или нажмите кнопку Обзор для ее выбора.
3. Нажмите кнопку OK. Операционной системе Windows Server 2012 понадобится перезапустить службу DHCP-сервер. Когда система попросит разрешения это сделать, нажмите кнопку Да. Служба будет остановлена и запущена снова.

В службе DHCP-сервер есть система самоконтроля, проверяющая использование дискового пространства. По умолчанию максимальный размер всех журналов DHCP-сервера составляет 70 Мбайт. Размер каждого журнала составляет одну седьмую часть от этого пространства. При достижении сервером предела в 70 Мбайт или при превышении отдельным журналом выделенного для него пространства регистрация деятельности DHCP прекращается, пока не будут очищены файлы журналов или место не освободится каким-либо иным способом. Обычно это происходит в начале нового дня, когда сервер очищает файл журнала прошлой недели.

Ключи реестра, контролирующие объем журнала и другие параметры, находятся в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Следующие параметры управляют регистрацией событий:

- DhcpLogFilesMaxSize — максимальный размер всех журналов. Стандартное значение — 70 Мбайт;
- DhcpLogDiskSpaceCleanupInterval — частота проверки использования диска и очистки журнала. Стандартный интервал — 60 минут;

– DhcpLogMinSpaceOnDisk — порог свободного пространства, необходимый для записи в журнал. Если свободное пространство на диске меньше установленного значения, запись в журнал временно прекращается. Стандартное значение — 20 Мбайт.

Параметр DhcpLogMinSpaceOnDisk не создается автоматически. Необходимо создать его самостоятельно и задать подходящее для сети значение.

Интеграция DHCP и DNS Служба DNS используется для разрешения имен компьютеров в доменах Active Directory и Интернете. Благодаря протоколу динамического обновления DNS, администратор избавлен от необходимости регистрировать DHCP-клиентов в DNS вручную. Протокол позволяет клиенту или DHCP-серверу при необходимости регистрировать в DNS записи прямого и обратного просмотра. При работе DHCP по умолчанию DHCP-клиенты Windows Server 2012 автоматически обновляют соответствующие DNS-записи после получения IP-адреса в аренду. Записи клиентов, работающих в предыдущих версиях Windows, после предоставления аренды обновляются DHCP-сервером. Можно изменить этот порядок для DHCP- сервера в целом или для конкретной области.

Защита имен — дополнительная функция в Windows Server 2012. Благодаря защите имен, DHCP-сервер регистрирует записи от имени клиента, только если никакой другой клиент с этой DNS-информацией не зарегистрирован. Можно настроить защиту имени для IPv4 и IPv6 на уровне сетевого адаптера или на уровне области. Параметры защиты имен, настроенные на уровне области, имеют приоритет над параметрами на уровне IPv4 или IPv6.

Защита имени предназначена для предотвращения занятия имен. Занятие имен происходит, когда компьютер с ОС, отличной от Windows, регистрирует в DNS имя, которое уже используется на компьютере под управлением Windows. Включив защиту имен, можно предотвратить занятие имени не-Windows-компьютерами. Хотя занятие имени не представляет собой проблему при использовании Active Directory, лучше все-таки включить защиту имен во всех Windows-сетях.

Защита имени основана на идентификаторе конфигурации динамического узла (Dynamic Host Configuration Identifier, DHCID) и поддержке записи ресурса DHCID (DHCID RR) в DNS. Запись DHCID RR — это запись ресурса, хранимая в DNS и сопоставляющая имена для предотвращения дублированной регистрации. Запись ресурса используется службой DHCP для хранения идентификатора компьютера и других сведений об имени, например записи A/AAAA компьютера. Сервер DHCP может запросить сравнение и отклонить регистрацию компьютера с другим адресом, пытающегося зарегистрировать имя с существующей записью DHCID.

Можно просмотреть и изменить параметры глобальной DNS-интеграции так:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, щелкните правой кнопкой мыши на узле IPv4 или IPv6 и выберите команду Свойства.
2. Перейдите на вкладку Служба DNS (DNS). На рис. 15.3 показаны значения DNS- интеграции по умолчанию для IPv4 и IPv6. Поскольку параметры настроены по умолчанию, обычно их не нужно модифицировать.
3. При желании можно включить или выключить функцию защиты имен. При включенной защите имен DHCP-сервер регистрирует записи о клиенте, если никакой другой клиент с этой DNS-информацией не зарегистрирован. Для включения или отключения защиты имен нажмите кнопку Настроить (Configure). В окне Защита имен (Name Protection) установите или сбросьте флажок Включить защиту имен (Enable name protection) и нажмите кнопку OK.

Интеграция DHCP и NAP

Протокол защиты сетевого адреса (Network Address Protection, NAP) разработан для защиты сети от клиентов, не имеющих достаточных собственных средств защиты. Простейший способ включить NAP на DHCP — настроить DHCP-сервер как сервер политики сети (Network Policy Server, NPS). Для этого нужно установить роль Сервер политики сети (Network Policy Server), настроить политику объединения DHCP и NAP и включить NAP на DHCP.

При этом на сетевых компьютерах осуществляется включение NAP, но не его настройка. Интегрировать NAP и DHCP можно так:

1. На сервере, который будет функционировать как сервер политики сети, используя мастер добавления ролей и компонентов, нужно установить как минимум роль Сервер политики сети.

2. Из меню Средства диспетчера серверов выберите команду Сервер политики сети (Network Policy Server), выберите узел NPS (локально) (NPS (Local)), нажмите кнопку Настройка (NAP) (Configure NAP) на главной панели. Будет запущен мастер Настройка NAP (Configure NAP Wizard).

3. Из списка Способ сетевого подключения (Network connection method) выберите Протокол DHCP (Dynamic Host Configuration Protocol (DHCP)). Имя политики по умолчанию будет NAP DHCP. Нажмите кнопку Далее.

4. На странице Укажите серверы принудительной защиты доступа к сети под управлением DHCP-сервера (Specify NAP Enforcement Servers Running DHCP Server) нужно указать все DHCP-серверы в сети.

- Нажмите кнопку Добавить. В окне Новый RADIUS-клиент (New RADIUS Client) введите имя удаленного сервера в поле Понятное имя (Friendly name). Затем введите DNS-имя удаленного DHCP-сервера в поле Адрес (Address). Нажмите кнопку Проверить (Verify), чтобы проверить адрес.
- На панели Общий секрет (Shared Secret) выберите переключатель Создать (Generate), чтобы создать длинный пароль с общим секретом. Нужно будет ввести эту фразу в политику NAP DHCP на всех удаленных DHCP-серверах. Поэтому обязательно запишите ее или сохраните в файле, в безопасном месте. Можно также скопировать эту фразу в Блокнот и сохранить в безопасном расположении. Нажмите кнопку OK.

5. Нажмите кнопку Далее. На странице Укажите DHCP-области (Specify DHCP Scopes) можно задать DHCP-области, к которым будет применена политика. Если области не указаны, политика применяется ко всем областям на выбранных DHCP-серверах, на которых включена NAP. Нажмите кнопку Далее дважды для пропуска страницы Группы компьютеров (Configure Machine Groups).

6. На странице Задайте группу сервера исправлений NAP и URL-адрес (Specify A NAP Remediation Server Group And URL) нажмите кнопку Создать группу (New Group) для определения группы серверов исправлений. На этих серверах хранятся обновления программного обеспечения для NAP-клиентов. В предоставленное текстовое поле введите URL веб-страницы с инструкцией, как привести компьютер в соответствие с политикой NAP. Убедитесь, что клиенты DHCP могут открыть эту страницу. Нажмите кнопку Далее.

7. На странице Определите политику работоспособности NAP (Define NAP Health Policy) укажите, как будет работать политика работоспособности NAP. В большинстве случаев можно оставить параметры по умолчанию, запрещающие вход в сеть клиентам, которые не совместимы с NAP. Для NAP-совместимых клиентов будет проводиться проверка работоспособности и автоматическое исправление, что позволяет им получать необходимые обновления программного обеспечения. Нажмите кнопку Далее, а затем кнопку Готово.

Можно настроить параметры NAP для всего сервера или для отдельных областей. Для просмотра или изменения глобальных параметров NAP выполните следующие действия:

1. В консоли DHCP разверните узел необходимого DHCP-сервера. Щелкните правой кнопкой мыши по узлу IPv4 и выберите команду Свойства.
2. На вкладке Защита доступа к сети (Network Access Protection) (рис. 15.5) нажмите кнопку Включить во всех областях (Enable on all scopes) или кнопку Отключить во всех областях (Disable on all scopes), чтобы включить или выключить NAP для всех областей сервера. Когда локальный DHCP-сервер также является сервером NAP, NAP-сервер всегда должен быть доступен. Если сервер не настроен, как сервер сетевой политики, или сервер DHCP неспособен связаться с заданным NAP-сервером, на вкладке Защита доступа к сети будет отображено сообщение об ошибке.
3. Выберите следующие опции, чтобы указать, как должен действовать DHCP-сервер, если NPS-сервер недоступен. Затем нажмите кнопку OK для сохранения параметров.
   - Полный доступ (Full Access) — предоставляет DHCP-клиентам полный (неограниченный) доступ к сети. Клиентам позволено выполнять любые разрешенные действия.
   - Ограниченный доступ (Restricted Access) — предоставляет DHCP-клиентам ограниченный доступ к сети. Клиенты могут работать только с тем сервером, к которому они подключены.
   - Отбросить клиентский пакет (Drop Client Packet) — блокирует запросы клиентов и запрещает выход клиентов в сеть. У клиентов нет доступа к ресурсам сети.

Для просмотра и изменения параметров NAP для отдельных областей выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Затем разверните узел IPv4.
2. Щелкните правой кнопкой мыши по нужной области и выберите команду Свойства.
3. На вкладке Защита доступа к сети установите переключатель Включить для этой области (Enable For This Scope) или Отключить для этой области (Disable For This Scope), чтобы включить или отключить NAP для данной области.
4. Если NAP включен и нужно использовать профиль NAP, отличный от стандартного, установите переключатель Использовать особый профиль (Use Custom Profile) и введите имя профиля, например Alternate NAP DHCP.
5. Нажмите кнопку OK для сохранения параметров.

Как избежать конфликтов IP-адресов

Часто причиной проблем с DHCP становятся конфликты IPv4-адресов. Двум компьютерам в сети нельзя иметь один IP-адрес. Если компьютеру

назначен уже использованный IPv4-адрес, один или оба компьютера могут быть отключены от сети. Точнее, компьютер, уже использующий IPv4-адрес, будет и дальше его использовать, а любой другой компьютер, который пытается использовать этот же адрес, будет блокирован от его использования. Чтобы своевременно обнаруживать конфликты, а еще лучше, избежать их, включите обнаружение конфликтов IPv4-адресов, выполнив следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой мыши по узлу IPv4 и выберите команду Свойства.
2. На вкладке Дополнительно присвойте параметру Число попыток определения конфликтов (Conflict Detection Attempts) отличное от нуля значение. Оно определяет количество проверок IP-адреса, которые DHCP-сервер проводит перед предоставлением адреса клиенту. Сервер DHCP проверяет IP-адреса, отправляя по сети запросы PING.

Одиночный (unicast) IP-адрес — это стандартный IP-адрес для сетей классов A, B и C. Когда DHCP-клиент запрашивает аренду, DHCP-сервер проверяет свой пул на наличие свободных адресов и назначает клиенту аренду на доступном IPv4-адресе. По умолчанию сервер проверяет список текущих аренд для определения, свободен ли адрес. Он не опрашивает физически сеть, чтобы узнать, используется ли адрес. К сожалению, в больших загруженных сетевых окружениях администраторы могут назначить этот IPv4-адрес другому компьютеру или оффлайн-компьютер может появиться в сети с арендой, которая еще не просрочена, даже если DHCP-сервер считает, что ее срок уже истек. Чтобы уменьшить конфликты этих типов, установите значение для параметра Число попыток определения конфликтов больше 0.

Сохранение и восстановление конфигурации DHCP

После того как будут установлены все необходимые DHCP-параметры, нужно сохранить конфигурацию DHCP так, чтобы можно было впоследствии ее восстановить на DHCP-сервере. Для сохранения конфигурации введите следующую команду в командной строке:

netsh dump DHCP >dhcpconfig.dmp

В этом примере dhcpconfig.dmp — имя сценария конфигурации. После создания этого сценария восстановить конфигурацию можно с помощью следующей команды, введенной в командной строке:

netsh exec dhcpconfig.dmp

Также можно использовать эту технику для настройки другого DHCP-сервера с такой же конфигурацией. Просто скопируйте сценарий конфигурации в папку на другом сервере и выполните его.

Можно сохранить и восстановить конфигурацию DHCP и с помощью консоли DHCP. Для сохранения конфигурации щелкните правой кнопкой

мыши на записи DHCP-сервера, выберите команду Архивировать (Backup), а в открывшемся окне выберите папку для архива и нажмите кнопку OK. Для восстановления конфигурации щелкните правой кнопкой мыши на записи сервера и выберите команду Восстановить (Restore). Используя открывшееся окно, выберите архивную папку и нажмите кнопку OK. Нажмите кнопку Да для подтверждения своих намерений.

Управление областями DHCP

После установки DHCP-сервера нужно настроить области, которые сервер DHCP будет использовать. Области — это пул IP-адресов, которые могут быть переданы в аренду клиентам. Как было рассказано ранее в разд. "Области адресов", для IPv4 можно создать суперобласти, обычные, многоадресные и отказоустойчивые области, для IPv6 можно создать только обычные области.

Суперобласти: создание и управление

Суперобласть служит контейнером для областей IPv4 так же, как и организационное подразделение является контейнером для объектов Active Directory. Суперобласти помогают управлять имеющимися в сети областями и также обеспечивают поддержку DHCP-клиентов в одной физической сети, где используются множественные логические IP-сети или же когда создаете суперобласти для распространения IP-адресов из разных логических
сетей в один сегмент физической сети. С помощью суперобласти можно активировать или деактивировать сразу несколько областей. Также в суперобласти можно просматривать статистику для всех областей сразу, вместо того чтобы проверять статистику для каждой области отдельно.

Создание суперобластей

После создания как минимум одной обычной или многоадресной IPv4-области можно создать суперобласть так:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, а затем щелкните правой кнопкой мыши по узлу IPv4, выберите команду Создать суперобласть (New Superscope) (эта команда появится, если есть хотя бы одна обычная или многоадресная область). Будет запущен мастер создания суперобласти (New Superscope Wizard). Нажмите кнопку Далее.
2. Выберите имя суперобласти и нажмите кнопку Далее.
3. Выберите области, которые нужно добавить в суперобласть. Для выбора области просто щелкните на ней в списке Доступные области (Available Scopes). Чтобы выбрать несколько областей, щелкните по ним при нажатых клавишах <Shift> или <Ctrl>.
4. Нажмите кнопку Далее, а затем кнопку Готово.

Добавление областей в суперобласть

Добавлять области в суперобласть можно как в процессе ее создания, так и позже. Чтобы добавить область в существующую суперобласть, выполните следующие действия:

1. Правой кнопкой мыши щелкните на области, которую хотите добавить в существующую суперобласть, и выберите команду Добавить в суперобласть (Add To Superscope).
2. В диалоговом окне Добавление области к суперобласти (Add Scope To A Superscope) выберите суперобласть.
3. Нажмите кнопку OK.

Удаление областей из суперобласти

Для удаления области из суперобласти выполните следующие действия:

1. Щелкните правой кнопкой мыши на области, которую нужно удалить из суперобласти, и выберите команду Удалить из суперобласти (Remove From Superscope).
2. Нажмите кнопку Да, чтобы подтвердить действие. Если это была последняя область, суперобласть будет автоматически удалена.

Включение и отключение суперобласти

При включении или отключении суперобласти также включаются или отключаются сразу все входящие в нее области. Для включения области щелкните на ней правой кнопкой мыши и выберите команду Активировать (Activate). Для отключения суперобласти щелкните на ней правой кнопкой мыши и выберите команду Деактивировать (Deactivate).

Удаление суперобласти

При удалении суперобласти удаляется только ее контейнер, но не сами области. Если нужно удалить области, которые входят в состав суперобласти, нужно сделать это отдельно. Для удаления суперобласти щелкните на ней правой кнопкой мыши и выберите команду Удалить (Delete). Нажмите кнопку Да для подтверждения своих намерений.

Создание областей и управление ими

Область предоставляет пул адресов для DHCP-клиентов. Обычная область — это область с адресами сетей классов A, B или C. Многоадресная область — это область с адресами сетей класса D. Хотя обычные и многоадресные области создаются по-разному, в управлении они мало чем отличаются друг от друга. Основное отличие состоит в том, что многоадресные области не позволяют резервировать адреса, а также задавать дополнительные параметры WINS, DNS, маршрутизации и т. д.

Создание обычной области для IPv4-адресов

Создать обычную область для IPv4-адресов можно с помощью следующих действий:

1. В консоли DHCP разверните узел сервера, с которым нужно работать, далее щелкните правой кнопкой мыши на узле IPv4. Если необходимо автоматически добавить новую область в суперобласть, выделите ее, а затем щелкните правой кнопкой мыши на нужной суперобласти.
2. В контекстном меню выберите команду Создать область (New Scope). Будет запущен мастер создания области (New Scope Wizard). Нажмите кнопку Далее.
3. Введите имя и описание области, а затем нажмите кнопку Далее.
4. Введите начальный и конечный адреса области в поля Начальный IP-адрес (Start IP address) и Конечный IP-адрес (End IP address) на странице Диапазон адресов (IP Address Range). Как правило, не нужно включать в область адреса x.x.x.0 и x.x.x.255, которые обычно зарезервированы для сетевых адресов и широковещательных сообщений соответственно. Поэтому необходимо использовать адреса от 192.168.10.1 до 192.168.10.254 вместо 192.168.10.0—192.168.10.255.
5. После указания диапазона IP-адресов поля Длина (Length) и Маска подсети (Subnet mask) будут заполнены автоматически. Если подсети не используются, оставьте стандартные значения.
6. Нажмите кнопку Далее. Если введенный диапазон IP-адресов охватывает разные сети, будет предоставлена возможность создать суперобласть, содержащую различные области для каждой сети. Нажмите кнопку Да, чтобы принять это предложение, и перейдите к шагу 8. Если была допущена ошибка, нажмите кнопку Назад (Back), чтобы исправить введенный диапазон IP-адресов.
7. Используйте поля Начальный IP-адрес (Start IP address) и Конечный IP-адрес (End IP address) на странице Добавление исключений и задержка (Add Exclusions and Delay), чтобы определить диапазоны IP-адресов, которые будут исключены из области. Можно исключить диапазоны адресов так.
   - Для определения диапазона введите начальный и конечный адреса в поля Начальный IP-адрес (Start IP address) и Конечный IP-адрес (End IP address) и нажмите кнопку Добавить. Чтобы исключить один IP-адрес, введите его и как начальный, и как конечный IP-адрес.
   - Исключенные диапазоны адресов отображаются в списке Исключаемый диапазон адресов (Excluded address range).

- Для удаления диапазона исключения выберите его в списке Исключаемый диапазон адресов (Excluded address range) и затем нажмите кнопку Удалить.

8. Нажмите кнопку Далее. Укажите продолжительность аренды для диапазона адресов, используя поля Дней (Day(s)), часов (Hour(s)), минут (Minutes). Продолжительность аренды по умолчанию составляет 8 дней. Нажмите кнопку Далее. Слишком длительный срок аренды IP-адреса может снизить эффективность DHCP и стать причиной преждевременного исчерпания диапазона доступных IP-адресов, особенно в сетях с мобильными пользователями и другими типами компьютеров, которые не являются постоянными членами сети. Достаточная продолжительность аренды для большинства сетей - до 3 дней.
9. У администратора есть возможность настроить общие параметры DHCP для DNS, WINS, шлюзов и т. д. Если нужно настроить эти параметры сейчас, выберите переключатель Да, настроить эти параметры сейчас (Yes, I want to configure these options now). В противном случае выберите Нет, настроить эти параметры позже (No, I will configure these options later) и пропустите шаги 10—15.
10. Нажмите кнопку Далее. Первым делом необходимо указать основной шлюз. В поле IP-адрес введите IP-адрес основного шлюза и нажмите кнопку Добавить. Повторите этот процесс для других шлюзов по умолчанию.
11. Сначала клиенты будут использовать первый шлюз в списке. Если он недоступен, клиенты попытаются получить доступ к следующему шлюзу и т. д. С помощью кнопок Вверх (Up) и Вниз (Down) можно изменять порядок шлюзов.
12. Нажмите кнопку Далее. Настройте параметры DNS для DHCP-клиентов. Введите имя родительского домена, который следует использовать для разрешения не полностью определенных имен компьютеров. для настройки параметров DNS по умолчанию для DNS-клиентов
13. В поле IP-адрес введите IP-адрес основного DNS-сервера, а затем нажмите кнопку Добавить. Повторите этот процесс, чтобы указать дополнительные серверы. Здесь опять же порядок записей определяет, какой из IP-адресов будет использован в первую очередь. При необходимости, измените порядок с помощью кнопок Вверх и Вниз. Нажмите кнопку Далее. Если знаете имя сервера, вместо IP-адреса можно ввести его в поле Имя сервера (Server name), а затем нажмите кнопку Сопоставить (Resolve). После этого добавьте IP-адрес сервера, нажав кнопку Добавить.
14. Параметры WINS задаются аналогично. Нажмите кнопку Далее.

15. Если нужно активировать область, установите переключатель Да, я хочу активировать эту область сейчас (Yes, I want to activate this scope now). В противном случае установите переключатель Нет, я активирую эту область позже (No, I will activate this scope later).

Создание обычной области для IPv6-адресов

Создать обычную область для IPv6-адресов можно с помощью мастера создания области. При настройке DHCP для IPv6 нужно ввести идентификатор сети и предпочтительное значение. Обычно первые 64 бита IPv6-адреса идентифицируют сеть, и это 64-битное значение нужно ввести в окне мастера создания области. Предпочитаемое значение устанавливает приоритет этой области относительно других областей. Область с наименьшим предпочитаемым значением будет использована первой. Далее будет использована область со вторым наименьшим значением и т. д. Создать обычную область для IPv6-адресов можно с помощью следующих действий:

1. В консоли DHCP разверните узел сервера, с которым нужно работать.
2. Щелкните правой кнопкой мыши на узле IPv6. Из появившегося контекстного меню выберите команду Создать область. Будет запущен мастер создания области. Нажмите кнопку Далее.
3. Введите имя и описание области, а затем нажмите кнопку Далее.
4. На странице Префикс области (Scope Prefix) (рис. 15.8) введите 64-битный префикс сети и затем установите предпочтение. Нажмите кнопку Далее.
5. Используйте поля Начальный IPv6-адрес и Конечный IPv6 адрес на странице Добавление исключений (Add Exclusions) для определения диапазонов IPv6-адресов, которые должны быть исключены из диапазона. Исключить несколько диапазонов можно так.
   - Чтобы определить диапазон исключения, в разделе Исключенный диапазон адресов (Exclusion Range) введите начальный и конечный адреса в поля Начальный IPv6-адрес и Конечный IPv6-адрес и нажмите кнопку Добавить. Чтобы исключить один IPv6-адрес, введите его как начальный IPv6-адрес и нажмите кнопку Добавить.
   - Отследить исключенные диапазоны адресов можно в списке Исключенный диапазон адресов (Excluded Address Range).
   - Чтобы удалить исключение, выделите диапазон в списке Исключенный диапазон адресов (Excluded Address Range) и нажмите кнопку Удалить.
6. Нажмите кнопку Далее. Динамические IPv6-адреса могут быть временными и постоянными. Постоянный адрес похож на зарезервированный адрес. На странице Аренда области (Scope Lease)

укажите сроки аренды для временных и постоянных адресов в разделах Основное время жизни (Preferred Life Time) и Допустимое время жизни (Valid Life Time). Основное время жизни — это типичный интервал, в течение которого будет действительна аренда. Допустимое время жизни — это максимальный интервал, в течение которого будет действительна аренда. Нажмите кнопку Далее. Слишком длительный срок аренды IP-адреса может снизить эффективность DHCP и стать причиной преждевременного исчерпания диапазона доступных IP-адресов, особенно в сетях с мобильными пользователями и другими типами компьютеров, которые не являются постоянными членами сети. Достаточная продолжительность постоянной аренды — от 8 до 30 дней.

7. Если нужно активировать область, выберите переключатель Да на панели Активировать область сейчас (Activate Scope Now), а затем нажмите кнопку Готово. В противном случае выберите переключатель Нет и нажмите кнопку Готово.

Создание многоадресных областей

Для создания многоадресной области выполните следующие действия:

1. В консоли DHCP разверните узел сервера, с которым нужно работать. Выберите и затем щелкните правой кнопкой мыши на узле IPv4. Если необходимо добавить новую область в суперобласть, вместо этого выберите и щелкните правой кнопкой мыши на суперобласти.
2. Из контекстного меню выберите команду Создать многоадресную область (New Multicast Scope). Будет запущен мастер создания многоадресной области (New Multicast Scope Wizard). Нажмите кнопку Далее.
3. Введите имя и описание области, а затем нажмите кнопку Далее.
4. Поля Начальный IP-адрес и Конечный IP-адрес определяют допустимый диапазон IP-адресов для области. Введите начальный и конечный адреса в эти поля. Необходимо определить многоадресную область, используя IP-адреса класса D. Это означает, что допустимый диапазон IP-адресов — от 224.0.0.0 до 239.255.255.255.
5. Сообщения, посылаемые компьютерами при помощи многоадресных IP-адресов, имеют определенное время жизни (Time to Live, TTL). Им определяется максимальное количество маршрутизаторов, через которые может пройти сообщение. Стандартное значение TTL равно 32. В большинстве сетей этого достаточно. Если имеется большая сеть, увеличьте это значение, чтобы оно соответствовало реальному количеству маршрутизаторов.
6. Нажмите кнопку Далее. Если была допущена ошибка, нажмите кнопку Назад и измените указанный диапазон IP-адресов.

7. На странице Добавление исключений (Add Exclusions) задайте диапазоны IP-адресов, которые следует исключить из области. Можно исключить несколько диапазонов.
   - Чтобы определить исключаемый диапазон, введите начальный и конечный адреса в поля Начальный IP-адрес и Конечный IP-адрес и нажмите кнопку Добавить.
   - Отследить исключенные диапазоны адресов можно в списке Исключаемые адреса.
   - Чтобы удалить исключенный диапазон, выделите диапазон в списке Исключаемые адреса и нажмите кнопку Удалить.
8. Нажмите кнопку Далее. Укажите продолжительность аренды для области в днях, часах и минутах. По умолчанию продолжительность аренды составляет 30 дней. Нажмите кнопку Далее. Если нет богатого опыта работы с многоадресной передачей, не нужно изменять стандартное значение продолжительности аренды. Способ использования многоадресной аренды отличается от обычной аренды. Многие компьютеры могут использовать многоадресные IP-адреса и все эти компьютеры могут арендовать IP-адрес. Хорошая продолжительность многоадресной аренды для большинства сетей — от 30 до 60 дней.
9. Если нужно активировать область, выберите переключатель Да, а затем нажмите кнопку Далее. В противном случае выберите переключатель Нет и нажмите кнопку Далее.
10. Нажмите кнопку Готово для завершения процесса.

Установка параметров области

Параметры области позволяют точно контролировать функционирование области и установить настройки TCP/IP по умолчанию для клиентов, которые используют область. Например, можно использовать параметры области для автоматической установки адресов DNS-серверов на клиентах сети. Также можно определить основные шлюзы, WINS и многое другое. Параметры области применяются только к обычным областям, но не к многоадресным. Установить параметры области можно следующими способами:

- глобально для всех областей, задав параметры по умолчанию DHCP-сервера;
- отдельно для каждой области путем установки ее параметров;
- отдельно для каждого клиента путем установки параметров резервирования;
- для класса клиентов путем настройки класса пользователей.

У областей IPv4 и IPv6 — разные параметры. Параметры области используют иерархию для определения применения тех или иных

параметров. Предыдущий список показывает эту иерархию. В общем, она объясняет следующее:

- параметры, заданные для конкретной области, перезаписывают глобальные параметры;
- параметры клиента перезаписывают параметры области и глобальные параметры;
- параметры класса клиента перезаписывают все другие параметры.

Просмотр и назначение параметров сервера

Параметры сервера применяются ко всем настроенным областям на определенном DHCP-сервере. Можно просмотреть и задать эти параметры так:

1. В консоли DHCP дважды щелкните на сервере, параметры которого нужно изменить, а затем разверните его узлы IPv4 и IPv6 в дереве консоли.
2. Чтобы просмотреть его текущие параметры, выберите узел Параметры сервера (Server Options), который находится или в узле IPv4, или в узле IPv6 в зависимости от того, с каким типом адреса нужно работать. Текущие параметры будут отображены на правой панели.
3. Чтобы назначить новые параметры сервера, щелкните правой кнопкой мыши по узлу Параметры сервера и из контекстного меню выберите команду Настроить параметры (Configure Options). Откроется окно Параметры: сервер (Server Options). В области Доступный параметр (Available Options) отметьте флажком первую опцию, которую нужно настроить. Затем, когда она будет выбрана, введите требуемую информацию на панели Ввод данных (Data Entry). Повторите этот процесс для настройки всех остальных параметров.
4. Нажмите кнопку OK для сохранения изменений.

Просмотр и назначение параметров области

Параметры области применяются к отдельной области и переопределяют параметры сервера по умолчанию. Просмотреть и изменить параметры области можно так:

1. В консоли DHCP разверните запись области.
2. Для просмотра текущих параметров выберите узел Параметры области (Scope Options). На панели справа будут отображены заданные параметры.
3. Для назначения новых параметров щелкните правой кнопкой мыши на узле Параметры области и выберите команду Настроить параметры. В области Доступный параметр отметьте флажком первую опцию, которую нужно настроить. Затем, когда она будет

выбрана, введите требуемую информацию на панели Ввод данных (рис. 15.10). Повторите этот процесс для настройки всех остальных параметров.

4. Нажмите кнопку OK. и введите требуемую информацию в область Ввод данных

Просмотр и назначение параметров резервирования

Администратор может назначить параметры резервирования клиенту, у которого есть зарезервированные IPv6- или IPv4-адреса. Эти параметры закрепляются за конкретным клиентом и перекрывают параметры сервера и области. Чтобы просмотреть и изменить параметры резервирования, выполните следующие действия:

1. В консоли DHCP разверните запись области, с которой нужно работать.
2. Дважды щелкните на папке Резервирование (Reservations) для области.
3. Чтобы просмотреть текущие параметры, щелкните на нужном резервировании. Настроенные параметры будут отображены в правой панели.
4. Чтобы назначить новые параметры, щелкните правой кнопкой мыши на резервировании и выберите команду Настроить параметры. Откроется диалоговое окно Параметры: резервирование (Reservation Options). В разделе Доступный параметр установите флажок первого настраиваемого параметра и введите нужную информацию в поля раздела Ввод данных. Повторите этот шаг для настройки других параметров

Изменение областей

Изменить существующую область можно с помощью следующих действий:

1. В консоли DHCP дважды щелкните на сервере, с которым нужно работать, а затем разверните его узлы IPv4 или IPv6. Будут отображены области, настроенные для сервера.
2. Щелкните правой кнопкой мыши на области, которую нужно изменить, и выберите команду Свойства.
3. Теперь можно изменить параметры области. Имейте в виду следующее.
   - При изменении обычной области IPv4 у администратора есть возможность задать неограниченный срок аренды. Это негативно сказывается на эффективности выделения IP-адресов DHCP-сервером. Постоянная аренда не заканчивается, пока она не будет отключена физически или не будет отключена область. В результате возникает риск постепенно

исчерпать все адреса, в особенности при расширении сети. Лучшей альтернативой неограниченному сроку аренды является использование резервирований, причем только для тех клиентов, которые действительно нуждаются в постоянном IP-адресе.

- При изменении многоадресных областей у администратора есть возможность задать время жизни области. Оно определяет количество времени, в течение которого будет действительна область. По умолчанию многоадресные области действительны, пока они включены. Чтобы изменить этот параметр, перейдите на вкладку Время жизни многоадресной области (Lifetime), установите переключатель Срок действия многоадресной области истекает (Multicast scope expires on) и задайте срок действия.

Активация и деактивация областей

В консоли DHCP неактивная область помечается белым кружком с красной стрелкой вниз.
У активной области значок, как у обычной папки.
Чтобы активировать неактивную область, щелкните по ней правой кнопкой мыши в консоли DHCP и выберите команду Активировать. Чтобы деактивировать активную область, щелкните ее правой кнопкой мыши в консоли DHCP и выберите команду Деактивировать.
Деактивация выключает область, но не прекращает текущие аренды клиентов. Если нужно завершить аренды, следуйте инструкциям из разд. "Освобождение адресов и аренды" далее в этой главе.

Включение протокола BOOTP

Протокол BOOTP (Bootstrap Protocol) — протокол для динамической IPv4-адресации, который является предшественником DHCP. Нормальные области не поддерживают BOOTP. Чтобы включить поддержку BOOTP, выполните следующие действия:

1. Щелкните на обычной области для IPv4-адресов правой кнопкой мыши, а затем выберите команду Свойства.
2. На вкладке Дополнительно выберите переключатель обоих типов серверов (Both) для поддержки и DHCP-клиентов, и BOOTP-клиентов.
3. При необходимости установите продолжительность аренды для BOOT-клиентов и нажмите кнопку OK

Удаление области

Удаление области удаляет область из DHCP-сервера без возможности восстановления. Для удаления области выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши на области, которую нужно удалить, а затем выберите команду Удалить.
2. Для подтверждения действия нажмите кнопку Да.

Настройка нескольких областей в сети

Можно настроить несколько областей в одной сети. Один DHCP-сервер или несколько DHCP-серверов могут обслуживать эти области. Однако при работе с несколькими областями важно помнить, что диапазоны этих областей не должны накладываться. У каждой области должен быть уникальный диапазон адресов. Если это не так, одинаковые IP-адреса могут быть назначены разным DHCP-клиентам, что может вызвать серьезные проблемы в сети.

Чтобы понять, как можно использовать несколько областей, рассмотрим следующий сценарий, в котором каждый сервер имеет свою DHCP-область и обслуживает свой диапазон в одной и той же сети:

сервер A — 192.168.10.1—192.168.10.99;
сервер B — 192.168.10.100—192.168.10.199;
сервер C — 192.168.10.200—192.168.10.254.

Каждый из этих серверов отвечает на сообщения обнаружения DHCP и любой из них может назначить IP-адреса клиентам. Если один из серверов откажет, другие серверы могут продолжить предоставлять DHCP-услуги сети. Чтобы предоставить отказоустойчивость и избыточность, можно использовать области, как будет показано в следующем разделе.

Создание и управление отказоустойчивыми областями

Отказоустойчивые области разбиваются между двумя DHCP-серверами и повышают отказоустойчивость, предоставляют избыточность, а также обеспечивают балансировку нагрузки. Используя отказоустойчивую область, можно идентифицировать два DHCP-сервера, которые разделят область. Если один из серверов откажет или станет перегруженным, другой сервер может занять его место, продолжая назначать IP-адреса и возобновлять уже существующие аренды. Отказоустойчивая область помогает также и при балансировке нагрузки серверов.

Создание отказоустойчивой области

Отказоустойчивые области применяются только к IPv4-адресам. Можно разбить одну обычную область или суперобласть, содержащую несколько областей. Создавать отказоустойчивую область нужно на DHCP-сервере, который должен действовать как основной сервер. Такая область создается путем разделения существующей области или суперобласти. При создании отказоустойчивой области нужно определить сервер-партнер, с которым будет разделена область основного сервера. Этот дополнительный сервер действует как вторичный сервер для области. Поскольку отказоустойчивые

области — это улучшение со стороны серверов, никакая дополнительная настройка DHCP-клиентов не требуется.

Способ разделения области зависит от настроек отказоустойчивой области.

- Оптимизация для балансировки нагрузки. Для отказоустойчивой области, оптимизированной для балансировки нагрузки, установлена минимальная задержка (или вообще нет задержки) в ее свойствах. Без задержки и основной и вторичный серверы могут ответить на запросы DHCP DISCOVER от DHCP-клиентов. Это позволяет самому быстрому серверу отвечать на запрос и принимать DHCPOFFER первому. Если один из серверов станет недоступен или будет перегружен и не сможет ответить на запросы, другой сервер обработает запросы и продолжит назначение адресов, пока обычный процесс не будет восстановлен. Для балансировки нагрузки нужно установить режим балансировки нагрузки.
- Оптимизация для отказоустойчивости. Отказоустойчивая область, оптимизированная для отказоустойчивости, имеет довольно большую задержку в настройках области. Задержка на вторичных серверах позволяет серверу отвечать с задержкой на запросы DHCP DISCOVER от DHCP-клиентов. Задержка на вторичном сервере позволяет первичному серверу отвечать и принимать DHCPOFFER первому. Однако если основной сервер недоступен или перегружен и не может ответить на запрос, вторичный сервер обрабатывает запросы и продолжает распределять адреса, пока основной сервер снова не станет доступным. Для отказоустойчивости выберите режим горячей замены.

Создать отказоустойчивую область можно так:

1. В консоли DHCP подсоединитесь к основному DHCP-серверу отказоустойчивой области. Дважды щелкните на записи основного сервера, а затем разверните узел IPv4.
2. Область, с которой нужно работать, уже должна быть определена. Щелкните на обычной области или на суперобласти правой кнопкой мыши и выберите команду Настройка отработки отказа (Configure Failover). Откроется окно Настройка отработки отказа (Configure Failover Wizard). Нажмите кнопку Далее.
3. Затем нужно указать сервер-партнер. Нажмите кнопку Добавить сервер (Add Server). Используйте параметры окна Добавление сервера (Add Server), чтобы выбрать вторичный сервер для отказоустойчивой области, а затем нажмите кнопку OK. Сбросьте флажок Повторно использовать отношения отработки отказа, настроенные для этого сервера (Reuse existing failover relationships), а затем нажмите кнопку Далее для продолжения.

4. На странице Создайте новое отношение отработки отказа (Create A New Failover Relationship) (рис. 15.11) используйте раскрывающийся список Режим (Mode) для установки режима отказоустойчивости (Балансировка нагрузки (Load Balance) или Горячая замена (Hot Standby)).
5. Если выбран режим Балансировка нагрузки, используйте предоставленные параметры для установки того, как IP-адреса будут распределяться между каждым из серверов. Несколько примеров:
   - 80/20 — лучше всего работает, когда нужно, чтобы один из серверов обрабатывал большую часть нагрузки, а второй сервер заменял бы его в случае необходимости;
   - 60/40 — лучше, когда один из серверов обрабатывает немного больше нагрузки, но нужно, чтобы у обоих серверов была постоянная загрузка;
   - 50/50 — когда нужно одинаково распределить нагрузку между двумя серверами.
6. Если выбран режим Горячая замена, установите роль партнера — Активный (Active) или Резервный (Standby), а также укажите, сколько процентов адресов нужно зарезервировать. По умолчанию для сервера горячей замены резервируется 5% из диапазона адресов.
7. Заполните поле Общий секрет (Shared secret) для партнеров. Это специальный пароль, который партнеры используют при синхронизации DHCP-базы данных и осуществления других задач по обслуживанию отношений отработки отказа. Когда будете готовы продолжить, нажмите кнопку Далее.
8. Нажмите кнопку Готово. Просмотрите конфигурацию отказоустойчивой области. Если будут обнаружены какие-то ошибки, нужно внести соответствующие изменения. Нажмите кнопку Закрыть.

Модификация или удаление отказоустойчивых областей

Отказоустойчивые области не идентифицируются как таковые в консоли DHCP. Можно идентифицировать отказоустойчивую область по ее идентификатору сети и пулу IP-ад-ресов. Как правило, найти отказоустойчивую область очень просто: такая область будет на двух DHCP-серверах, а свойства области будут содержать информацию об обеспечении отказоустойчивости. Чтобы просмотреть эту информацию, щелкните правой кнопкой мыши область и выберите команду Свойства. В диалоговом окне Свойства перейдите на вкладку Отработка отказа (Failover).

Можно управлять отношения отработки отказа несколькими способами.

- Если есть подозрения, что конфигурация, относящаяся к отношениям отработки отказала, рассинхронизировалась, щелкните правой кнопкой мыши на области и выберите команду Репликация отношения (Replicate Partnership).
- Если есть подозрения, что база данных DHCP, которую совместно используют партнерские серверы, рассинхронизировалась, щелкните правой кнопкой мыши на области и выберите команду Репликация области (Replicate Scope).
- Если больше не нужно использовать отказоустойчивую область, щелкните правой кнопкой мыши по ней и выберите команду Удаление конфигурации отработки отказа (Deconfigure Failover).

Нельзя изменить параметры отношений отработки отказа. Однако можно сначала деконфигурировать отказоустойчивую область, а затем настроить ее заново.

Управление пулом адресов, арендами и резервированием

У областей есть отдельные папки для пула адресов, арендованных адресов и резервирования. В этих папках можно просмотреть текущую статистику для соответствующих данных и управлять существующими записями.

Просмотр статистики области

Статистика области предоставляет информацию о пуле адресов для текущей области или суперобласти. Чтобы просмотреть статистику, щелкните правой кнопкой мыши по области или суперобласти, а затем выберите команду Отобразить статистику (Display Statistics). Рассмотрим основные столбцы окна Статистика области (Scope Statistics):

- Всего областей (Total Scopes) — показывает, сколько областей в суперобласти;
- Всего адресов (Total Addresses) — сколько IP-адресов в области;
- Используется (In Use) — показывает (точное число и процентное соотношение используемых адресов по отношению к общему числу адресов), сколько адресов используется в данный момент. Если это значение достигает 85%, нужно задуматься о добавлении дополнительных адресов или освобождении уже используемых адресов;
- Доступен (Available) — общее число доступных адресов.

Включение и настройка фильтрации MAC-адресов

Фильтрация MAC-адресов — функция IPv4-адресов, которая позволяет включать или исключать компьютеры и устройства на основании их MAC-адресов. При настройке фильтрации MAC-адресов можно указать типы оборудования, которые освобождены от фильтрации. По умолчанию все типы оборудования, определенные в RFC 1700, освобождены от

фильтрации. Чтобы изменить льготы типа, выполните следующие действия:

- В консоли DHCP щелкните правой кнопкой мыши на узле IPv4, а затем выберите команду Свойства.
- На вкладке Фильтры (Filters) нажмите кнопку Дополнительно. В окне Дополнительные свойства фильтра (Advanced Filter Properties) с помощью флажков выберите типы оборудования, которые будут освобождены от фильтрации. Установите флажки типов оборудования, которые нужно фильтровать.
- Нажмите кнопку OK для сохранения изменений.

Перед настройкой фильтрации MAC-адресов нужно сделать следующее:

1. Включите и определите список адресов, которым разрешен доступ — список разрешенных. Сервер DHCP будет предоставлять доступ только тем DHCP-клиентам, MAC-адреса которых есть в этом списке. Любому клиенту, который ранее получил IP-адрес, будет отказано в возобновлении адреса, если его MAC-адреса нет в списке разрешенных.
2. Определите список запрещенных узлов. Сервер DHCP отказывает в обслуживании DHCP-клиентам, чьи MAC-адреса есть в списке запрещенных. Любому клиенту, который ранее получил IP-адрес, будет отказано в возобновлении адреса, если MAC-адрес есть в списке запрещенных узлов.
3. Список запрещенных имеет приоритет над списком разрешенных. Это означает, что DHCP-сервер предоставляет обслуживание только клиентам, MAC-адреса которых находятся в списке разрешенных, при условии, что нет никаких соответствий в списке запрещенных. Если MAC-адрес был запрещен, он будет заблокирован, даже если он находится в списке разрешенных.

Чтобы включить список разрешенных и запрещенных (или оба списка), выполните эти действия:

1. В консоли DHCP щелкните по узлу IPv4, а затем выберите команду Свойства.
2. На странице показана текущая конфигурация фильтра. Чтобы использовать список разрешенных, установите флажок Включить список разрешенных (Enable allow list). Чтобы включить список запрещенных, установите флажок Включить список запрещенных (Enable deny list).
3. Нажмите кнопку OK для сохранения изменений.

В качестве альтернативы можно просто щелкнуть правой кнопкой мыши по узлу Разрешить (Allow) или Запретить (Deny) в узле Фильтры (Filters) и выбрать команду Включить (Enable) для включения списка разрешенных или запрещенных. Если нужно отключить какой-то из этих список,

щелкните по списку правой кнопкой мыши и выберите команду Отключить (Disable).
После включения фильтрации нужно определить фильтры, используя MAC-адреса клиентских компьютеров или сетевых устройств. На клиентском компьютере можно получить его MAC-адрес с помощью команды ipconfig /all в командной строке. Запись Физический адрес (Physical Address) показывает MAC-адрес клиента. Необходимо точно ввести это значение, чтобы фильтр работал. MAC-адрес определяется как восемь двухзначных шестнадцатеричных чисел, разделенных дефисом, как показано здесь:
FE-01-56-23-18-94-EB-F2
При определении фильтра нужно указать MAC-адрес (с дефисами или без них). Это означает, что можно ввести FE-01-56-23-18-94-EB-F2 или FE0156231894EBF2.
Также можно использовать звездочку (*) в качестве маски. Чтобы указать, что любое значение может соответствовать определенной части MAC-адреса, используйте вместо нее *, например:
FE-01-56-23-18-94-*-F2
FE-*-56-23-18-94-*-*
FE-01-56-23-18-*-*-*
FE01*
Чтобы настроить фильтр MAC-адреса, выполните следующие действия:

1. В консоли DHCP дважды щелкните по узлу IPv4 и перейдите в раздел Фильтры (Filters).
2. Щелкните правой кнопкой мыши по узлу Разрешить или Запретить, в зависимости от того, какой тип фильтра нужно создать, а затем выберите команду Новый фильтр (New Filter).
3. Введите MAC-адрес в фильтр, а затем прокомментируйте его в поле Описание (при особом желании). Нажмите кнопку Добавить. Повторите шаг для других фильтров.
4. Нажмите кнопку Закрыть, когда закончите.

Установка нового диапазона исключений

Можно исключить IPv4- или IPv6-адреса из области, определив диапазон исключений. В областях может быть несколько диапазонов исключений.
Для определения исключений в области IPv4-адресов выполните следующие действия:

1. В консоли DHCP разверните нужную область, щелкните правой кнопкой мыши на узле Пул адресов (Address Pool) и выберите команду Диапазон исключения (New Exclusion Range).
2. Введите начальный и конечный адреса в поля Начальный IP-адрес и Конечный IP-адрес и нажмите кнопку Добавить. Указанный диапазон должен быть подмножеством диапазона текущей

области и в данный момент не должен использоваться. Повторите этот шаг для добавления других диапазонов исключений.

3. Завершив настройку, нажмите кнопку Закрыть.

Чтобы определить диапазон исключений в области IPv6-адресов, выполните следующие действия:

1. В консоли DHCP разверните нужную область, щелкните правой кнопкой мыши на папке Исключения (Exclusions), а затем выберите команду Диапазон исключения (New Exclusion Range).
2. Введите начальный и конечный адреса в поля Начальный IPv6-адрес и Конечный IPv6-адрес и нажмите кнопку Добавить. Указанный диапазон должен быть подмножеством диапазона текущей области и в данный момент не должен использоваться. Повторите этот шаг для добавления других диапазонов исключений.
3. Завершив настройку, нажмите кнопку Закрыть.

Если исключение больше не нужно, его можно удалить. Выберите папку Пул адресов (IPv4) или Исключения (IPv6), щелкните правой кнопкой мыши на исключении и выберите команду Удалить. В окне подтверждения нажмите кнопку Да.

Резервирование DHCP-адресов

Протокол DHCP позволяет назначать постоянные адреса клиентам несколькими способами.

Первый способ заключается в использовании переключателя Без ограничений (Unlimited), в диалоговом окне свойств области можно назначить постоянный адрес всем клиентам, использующим данную область. Второй способ заключается в резервировании DHCP-адреса для конкретного клиента. В результате резервирования сервер DHCP всегда назначает клиенту один и тот же IP-адрес, сохраняя возможность централизованного управления, в чем и состоит преимущество DHCP.

Чтобы зарезервировать IP-адрес для клиента, выполните следующие действия:

1. В консоли DHCP разверните область, с которой нужно работать, а затем щелкните правой кнопкой мыши на папке Резервирование (Reservations) и в контекстном меню выберите команду Создать резервирование (New Reservation).
2. В поле Имя клиента (Reservation name) введите короткое, но описательное имя клиента. Данное поле используется только для идентификации.
3. В поле IP-адрес (IP address) введите IPv4-адрес, который нужно зарезервировать для клиента.
4. Этот IP-адрес должен принадлежать допустимому диапазону выбранной области.

5. Поле MAC-адрес (MAC address) содержит аппаратный адрес сетевого адаптера клиентского компьютера. Чтобы получить MAC-адрес, введите команду ipconfig /all в командной строке клиентского компьютера. В пункте Физический адрес содержится MAC-адрес клиента. Нужно ввести это значение без ошибок, иначе резервирование не будет работать.
6. Введите необязательный комментарий в поле Описание (Description).
7. По умолчанию поддерживаются и DHCP-клиенты, и BOOTP-клиенты. Это очень удобно, и отказываться от этой возможности следует, только если нужно исключить определенный тип клиента.
8. Нажмите кнопку Добавить для создания резервирования. Повторите этот шаг для добавления других резервирований.
9. Нажмите кнопку Закрыть.

Чтобы зарезервировать IPv6-адрес для клиента, выполните следующие действия:

1. В консоли DHCP разверните нужную область и щелкните правой кнопкой мыши на папке Резервирование. В появившемся меню выберите команду Создать резервирование.
2. В поле Имя клиента введите короткое и понятное имя. Данное поле используется только для идентификации.
3. В поле IPv6-адрес (IPv6 address) введите IPv6-адрес, который хотите закрепить за клиентом.
4. Этот IP-адрес должен принадлежать допустимому диапазону выбранной области.
5. В поле уникального идентификатора устройства DUID (Device Unique Identifier) нужно ввести MAC-адрес сетевого адаптера клиентского компьютера. Чтобы узнать MAC-адрес, введите команду ipconfig /all в командной строке клиентского компьютера.
6. В пункте Физический адрес хранится MAC-адрес клиента. Необходимо ввести это значение без ошибок, иначе резервирование не будет работать.
7. Идентификатор IAID (Identity Association Identifier) устанавливает уникальный префикс идентификатора клиента. Как правило, это значение состоит из 9 цифр.
8. При желании в поле Описание введите комментарий.
9. Нажмите кнопку Добавить, чтобы создать резервирование. Повторите этот процесс, чтобы добавить другие резервирования.
10. Когда закончите, нажмите кнопку Закрыть.

Освобождение адресов и аренды

При работе с зарезервированными адресами помните о двух нюансах.

- Зарезервированные адреса не переназначаются автоматически. Чтобы передать используемый адрес другому клиенту, адрес придется освободить. Для освобождения адреса аннулируйте аренду или введите на клиентском компьютере команду ipconfig /release.
- Клиенты не переходят на зарезервированные адреса автоматически. Если клиент уже использует некий IP-адрес, нужно заставить его освободить текущую аренду и запросить новую. Чтобы освободить адрес, аннулируйте аренду или введите на клиентском компьютере команду ipconfig /renew.

Изменение свойств резервирования

Изменить свойства резервирования можно с помощью следующих действий:

1. В консоли DHCP разверните область, с которой нужно работать, а затем перейдите в папку Резервирование (Reservations).
2. Щелкните правой кнопкой мыши на резервировании и выберите команду Свойства. После этого можно изменить параметры резервирования. Нельзя изменять неактивные параметры, зато можно изменить все остальные параметры. Эти параметры такие же, как были описаны в предыдущем разделе.

Удаление аренды и резервирования

Удалить активные аренды и резервирования можно так:

1. В консоли DHCP разверните область, с которой нужно работать, а затем перейдите в папку Арендованные адреса (Address Leases) или Резервирование.
2. Щелкните правой кнопкой мыши на аренде или резервировании и выберите команду Удалить.
3. Нажмите кнопку Да для подтверждения своих намерений.
4. После этого аренда или резервирование будут удалены из DHCP. Однако клиент после этого еще не освободит IP-адрес. Чтобы клиент освободил полученный IP-адрес, зарегистрируйтесь в его системе и введите команду ipconfig /release в командной строке.

Резервное копирование и восстановление базы данных DHCP

Серверы DHCP хранят DHCP-аренды и информацию резервирования в файлах базы данных. По умолчанию эти файлы находятся в каталоге %SystemRoot%\System32\DHCP. Основные фалы, находящиеся в этом каталоге:

- Dhcp.mdb — основной файл базы данных DHCP-сервера;

- J50.log — журнал транзакции, используемый для восстановления незавершенных транзакций в случае сбоя сервера;
- J50.chk — файл контрольной точки, используемый при усечении журнала регистрации транзакций DHCP-сервера;
- J500000A.log, J500000B.log, J500000C.log, J500000D.log, J500000E.log, J500000F.log — журналы резервирования для DHCP-сервера;
- Tmp.edb — временный рабочий файл DHCP-сервера.

Резервное копирование базы данных DHCP

Папка %SystemRoot%\System32\DHCP\Backup содержит резервные копии конфигурации и базы данных DHCP. По умолчанию база данных DHCP архивируется каждые 60 минут автоматически. Чтобы вручную сделать резервную копию базы данных DHCP, выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши на сервере, который нужно заархивировать, и выберите команду Архивировать (Backup).
2. В окне Обзор папок (Browse for folder) выберите папку, в которую нужно поместить резервную копию DHCP, а затем нажмите кнопку OK.

Параметры реестра, управляющие расположением архива, расписанием архивации, а также другими параметрами архивации DHCP, хранятся в разделе:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters Следующие параметры управляют базой данных DHCP и параметрами архивации:

- BackupDatabasePath — расположение базы данных DHCP. Этот параметр задается в окне свойств сервера DHCP. Перейдите на вкладку Дополнительно и установите нужное значение в поле Путь к базе данных (Database path);
- DatabaseName — имя основного файла базы данных DHCP. Значение по умолчанию — DHCP.mdb;
- BackupInterval — интервал архивации в минутах. Значение по умолчанию — 60 минут;
- DatabaseCleanupInterval — интервал очистки записей в базе данных. Значение по умолчанию — 4 часа.

Восстановление базы данных DHCP из резервной копии

В случае отказа сервера нужно восстановить и затем согласовать базу данных DHCP. Для восстановления базы данных DHCP из резервной копии выполните следующие действия:

1. Если нужно, восстановите из архива копию папки %SystemRoot%\System32\DHCP\ backup. Откройте консоль

DHCP, щелкните правой кнопкой мыши на сервере, который нужно восстановить, и выберите команду Восстановить (Restore).
2. В окне Обзор папок выберите папку, содержащую резервную копию, которую нужно восстановить, а затем нажмите кнопку OK.
3. Во время восстановления базы данных служба DHCP-сервер будет остановлена. В результате DHCP-клиенты временно не смогут получать IP-адреса.

Архивация и восстановление для перемещения базы данных DHCP на новый сервер

Если нужно перестроить сервер, предоставляющий службы DHCP, следует переместить DHCP-службы на другой сервер. Чтобы сделать это, нужно выполнить несколько действий на исходном и конечном серверах. На конечном сервере выполните следующее:

1. Установите службу DHCP-сервер на конечном сервере и перезагрузите сервер.
2. Остановите службу DHCP-сервер в консоли Службы.
3. Удалите содержимое папки %SystemRoot%\System32\DHCP.

На исходном сервере выполните следующие действия:

1. Остановите службу DHCP-сервер в консоли Службы.
2. После того как служба DHCP-сервер будет остановлена, отключите службу так, чтобы она больше не могла быть запущена.
3. Скопируйте содержимое папки %SystemRoot%\System32\DHCP исходного сервера в папку %SystemRoot%\System32\DHCP конечного сервера.

Теперь все необходимые папки находятся на конечном сервере. Запустите службу DHCP-сервер на конечном сервере, чтобы завершить перенос.

Принудительное регенерирование базы данных DHCP

Если база данных DHCP повреждена и Windows не в состоянии ее "починить" при переза-пуске службы DHCP-сервер, можно попытаться восстановить ее, как описано в разд. "Восстановление базы данных DHCP из резервной копии" ранее в этой главе. Если это не сработало, можно запуститься с новой копией базы данных DHCP так:

1. Остановите службу DHCP-сервер в консоли Службы.
2. Удалите содержимое папки %SystemRoot%\System32\DHCP, если нужно принудительно завершить регенерирование базы данных и запретить серверу восстановление из предыдущего архива. Также нужно удалить содержимое папки Backup. Не удаляйте DHCP-файлы, если ключи реестра DHCP-Server повреждены. Эти ключи должны быть доступны для восстановления базы данных DHCP.
3. Перезапустите службу DHCP-сервер.

4. В консоли DHCP не будут отображены аренды или другая информация для областей.
5. Чтобы вернуть активные аренды для каждой области, нужно согласовать области сервера, как будет показано в следующем разделе.
6. Чтобы предотвратить конфликты с ранее присвоенными арендами, нужно включить обнаружение конфликта адреса в течение следующих нескольких дней, как было показано ранее в этой главе.

Согласование аренд и резервирования

Согласование проверяет аренды клиентов и резервирования. Если будут найдены несогласованности между тем, что зарегистрировано в реестре Windows, и тем, что записано в базу данных DHCP-сервера, можно выбрать и согласовать любые противоречивые записи. Как только записи будут согласованы, DHCP восстановит IP-адрес для первоначального владельца или создаст временное резервирование для IP-адреса. Когда время аренды истечет, адрес будет восстановлен для будущего использования.

Можно согласовать области отдельно или же согласовать сразу все области на сервере. Для согласования отдельной области выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой мыши по области, с которой нужно работать, а затем выберите команду Согласование (Reconcile).
2. В окне Согласование (Reconcile) нажмите кнопку Проверить (Verify).
3. Если будут найдены противоречия, об этом сообщат. Выберите выведенные на экран адреса и нажмите кнопку Согласовать (Reconcile), чтобы избавиться от противоречий.
4. Если противоречий не будет, нажмите кнопку OK.

Чтобы согласовать все области на сервере, выполните следующие действия:

1. В консоли DHCP разверните запись сервера, затем щелкните правой кнопкой мыши на узле IPv4, выберите команду Согласовать все области (Reconcile All Scopes).
2. В окне Согласование всех областей (Reconcile All Scopes) нажмите кнопку Проверить.
3. Если будут найдены противоречия, об этом сообщат. Выберите выведенные на экран адреса и нажмите кнопку Согласовать, чтобы избавиться от противоречий.
4. Если противоречий не будет, нажмите кнопку OK.

ГЛАВА 3 Оптимизация DNS

В этой главе рассмотрены методы установки и управления системой доменных имен (DNS) в сети. DNS (Domain Name System) — это служба разрешения имен, преобразующая имена компьютеров в IP-адреса, позволяющие компьютерам находить друг друга. Система DNS работает через стек протоколов TCP/IP и может интегрироваться с WINS, DHCP и Active Directory. Полная интеграция DNS с сетевыми возможностями Microsoft Windows позволяет оптимизировать работу DNS в доменах Microsoft Windows Server.

Общие сведения о DNS

Система DNS объединяет группы компьютеров в домены. Эти домены организованы в иерархическую структуру, которая для публичных сетей определяется в Интернете, а для частных (также известных как интрасети или экстрасети) — на уровне предприятия. Различные уровни иерархии соответствуют отдельным компьютерам, доменам организаций и доменам верхнего уровня. В полностью определенном имени хоста omega.microsoft.com: omega — имя отдельного компьютера, microsoft — домен организации, com — домен верхнего уровня.

Домены верхнего уровня (Top Level Domains, TLD) лежат в основе иерархии DNS, поэтому их часто называют корневыми. Эти домены упорядочены географически, по типу организации и по назначению. Обычные домены, например microsoft.com, также называются родительскими доменами, поскольку являются родителями для групп или подразделений в организации. Можно разделить родительские домены на поддомены, предназначенные для групп или отделов внутри организации.

Поддомены часто называются дочерними доменами. Например, полное доменное имя (Fully Qualified Domain Name, FQDN) для компьютера из отдела кадров может называться jacob.hr.microsoft.com. Здесь jacob — имя узла, hr — дочерний домен, а microsoft.com — родительский домен.

Интеграция Active Directory и DNS

Как было упомянуто в главе 6, домены Active Directory используют DNS для реализации своей структуры имен и иерархии. Служба каталогов Active Directory и DNS настолько тесно взаимосвязаны, что перед установкой доменных служб Active Directory (AD DS) необходимо установить DNS в сети.

При установке первого контроллера домена в сети есть возможность автоматически установить DNS, если DNS-сервер не найден. Также можно указать, должны ли DNS и Active Directory полностью интегрироваться. В большинстве случаев на оба вопроса следует дать утвердительный ответ. При полной интеграции информация DNS хранится в Active Directory, что позволяет воспользоваться всеми преимуществами Active Directory. Важно понимать различия между частичной и полной интеграцией.

- Частичная интеграция. При частичной интеграции для хранения информации DNS используется стандартное хранилище. Информация DNS хранится в текстовых файлах с расширением dns в заданной по умолчанию папке %SystemRoot%\System32\Dns. Обновления DNS проводятся через единственный полномочный DNS-сервер. Этот сервер задан как основной DNS-сервер конкретного домена или области внутри домена, которая называется зоной (zone). Клиенты, использующие динамическое обновление DNS через DHCP, должны быть настроены на работу с основным DNS-сервером зоны. В противном случае DNS-информация на них обновляться не будет. Если в сети отсутствует основной DNS-сервер, проводить динамические обновления через DHCP нельзя.
- Полная интеграция. При полной интеграции информация DNS хранится в Active Directory, в контейнере dnsZone. Поскольку DNS-информация — это часть Active Directory, любой контроллер домена может получить доступ к данным, и динамические обновления через DHCP можно проводить по модели с несколькими хозяевами. А это позволяет любому контроллеру домена, на котором запущена служба DNS-сервер, обрабатывать динамические обновления. Клиенты, использующие динамические обновления DNS через DHCP, могут работать с любым DNS-сервером внутри зоны. Еще одно преимущество интеграции с каталогом заключается в возможности управлять доступом к DNS-информации при помощи системы безопасности каталога.

Если внимательно посмотреть на способ репликации информации DNS по сети, найдутся и другие преимущества полной интеграции с Active Directory. При частичной интеграции информация DNS хранится и реплицируется отдельно от Active Directory. Если есть две отдельные структуры, снижается эффективность как DNS, так и Active Directory, а также усложняется репликация. С точки зрения репликации изменений система DNS менее эффективна, чем Active Directory, поэтому репликация изменений DNS займет больше времени и ресурсов.

В предыдущих версиях DNS-сервера для Windows Server перезапуск DNS-сервера в больших организациях с большим числом зон, интегрированных в AD DS, мог длиться часами.

Это происходило потому, что данные зон загружались не в фоновом режиме одновременно с запуском службы DNS. В целях повышения эффективности DNS-серверов в Windows Server 2008 R2 и более поздних версиях они существенно доработаны. Теперь перезагрузки данных зон из AD DS осуществляются в фоновом режиме. Это гарантирует способность DNS-сервера отвечать на запросы, в том числе и из других зон.

При запуске DNS-сервер под управлением Windows Server 2008 R2 и более поздних версий выполняет следующие задачи:

- перечисляет все загружаемые зоны;
- загружает корневые ссылки из файлов или хранилища AD DS;
- загружает все зоны, хранящиеся в файлах, а не в AD DS;
- начинает отвечать на запросы и вызовы RPC (Remote Procedure Call);
- создает один или несколько потоков для загрузки зон, которые хранятся в AD DS.

Поскольку отдельные потоки загружают данные зоны, DNS-сервер способен во время загрузки зон отвечать на запросы. Если DNS-клиент посылает запрос относительно узла в уже загруженной зоне, DNS-сервер отвечает ему. Если это запрос относительно компьютера, который еще не загружен в память, сервер считывает данные узла из AD DS и соответствующим образом обновляет список записей.

Включение DNS в сети

Для включения DNS в сети нужно настроить DNS-клиенты и серверы. При настройке DNS-клиентов на них указываются IP-адреса DNS-серверов сети. Используя эти адреса, клиенты могут взаимодействовать с DNS-серверами по всей сети, даже если серверы находятся в разных подсетях.

Клиент DNS, встроенный в Windows 7 и Windows Server 2008 R2 и более поздние версии, поддерживает DNS-трафик по протоколам IPv4 и IPv6. По умолчанию при использовании протокола IPv6 серверам DNS назначаются хорошо известные локальные адреса FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2 и FEC0:0:0:FFFF::3. Чтобы добавить IPv6-адреса DNS-серверов используйте окно свойств протокола TCP/IPv6 или следующую команду:

netsh interface IPV6 ADD DNS

Серверы DNS, работающие под управлением Windows Server 2008 R2 или более поздних выпусков, в равной мере поддерживают протоколы IPv4 и IPv6. В консоли Диспетчер DNS (DNS Manager) адреса хостов отображаются как IPv4- или IPv6-адреса, соответственно.

Утилита командной строки Dnscmd также поддерживает оба формата. Теперь DNS-серверы способны посылать рекурсивные запросы на серверы с поддержкой только протокола IPv6,

тогда как список пересылки сервера может содержать и IPv4-, и IPv6-адреса. И наконец, DNS-серверы поддерживают доменное пространство имен для обратного просмотра.

Если сеть использует DHCP, его нужно настроить для работы с DNS. DCHP-клиенты могут регистрировать IPv6-адреса как вместе с IPv4-адресами, так и вместо них. Чтобы обеспечить надлежащую интеграцию DHCP и DNS, задайте параметры области DHCP. Для IPv4 нужно установить параметры области 006 DNS-серверы (006

DNS Servers) и 015 DNS-имя домена (015 DNS Domain Name). Для IPv6 следует установить параметры области 00023 Список адресов IPv6 рекурсивных серверов имен DNS (00023 DNS Recursive Name Server IPV6 Address) и 00024 Список поиска доменов (00024 Domain Search List). Также, если нужно организовать доступ к компьютерам сети из других доменов Active Directory, создайте для них записи в DNS. DNS-записи упорядочены по зонам — областям внутри домена.

DNS-клиенты под управлением Windows 7 (или более поздних версий), так же как и Windows Server 2008 R2, могут использовать протокол LLMNR (Link-Local Multicast Name Resolution) для разрешения имен в сегменте локальной сети, когда DNS-сервер недоступен.

Они также периодически производят поиск контроллера домена в домене, к которому они принадлежат. Такое поведение позволяет избежать проблем производительности, которые могут произойти, если отказ сети или сервера заставляет DNS-клиента связываться с удаленным контроллером домена, доступным по медленному соединению, а не с локальным контроллером домена. Ранее клиент использовал этот контроллер домена до тех пор, пока он не был вынужден искать новый контроллер, например, когда клиентский компьютер был долгое время отключен от сети. Периодически обновляя его связь с контроллером домена, DNS-клиент может уменьшить вероятность того, что он будет связан с несоответствующим контроллером домена

У службы DNS-клиент (DNS client) для Windows 8 и Windows Server 2012 есть несколько расширений безопасности относительно LLMNR и NetBIOS. Чтобы повысить безопасность для мобильных сетей, служба:

- не отправляет исходящие LLMNR-запросы по мобильной широкополосной (3G, EDGE) сети или по VPN-интерфейсам;
- не отправляет исходящие NetBIOS-запросы по мобильной широкополосной (3G, EDGE) сети.

Для лучшей совместимости с устройствами в энергосберегающем режиме тайм-аут LLMNR-запроса увеличен до 410 мс для первой попытки и 410 мс для второй попытки, что в сумме равно 820 мс вместо 300 мс. Чтобы улучшить время ответа для всех запросов, служба DNS-клиент делает следующее:

- параллельно отправляет LLNMR- и NetBIOS-запросы, оптимизируя их для IPv4 и IPv6;
- делит интерфейсы на сети для отправки параллельных DNS-запросов;
- использует асинхронный DNS-кэш с оптимизированным временем ответа.

Можно настроить DNS-клиент на компьютере под управлением Windows 7 или более поздней версии (или Windows Server 2008 R2 или более поздней версии) для нахождения ближайшего контроллера домена вместо

случайного поиска. В результате повысится производительность в сетях, содержащих домены, которые существуют по медленным соединениям. Однако поскольку этот процесс генерирует сетевой трафик, поиск ближайшего контроллера домена может отрицательно влиять на производительность сети.

В Windows Server 2008 и более поздних версиях поддерживаются основные зоны только для чтения и зона GlobalNames. Основная зона только для чтения автоматически создается для поддержки контроллера домена RODC. Когда компьютер становится RODC-контроллером, он реплицирует с доступом только для чтения полную копию всех разделов каталога приложений, используемых DNS, включая раздел домена, а также зоны DNS-леса (ForestDNSZones) и домена (DomainDNSZones). Это гарантирует наличие на DNS-сервере RODC полной копии всех зон DNS. Администратор RODC может просматривать содержимое основной зоны, но не может изменять его. Администратор может редактировать содержимое зоны только на стандартном контроллере домена.

Для поддержки всех сред DNS и разрешения однокомпонентных имен создается зона GlobalNames. Для оптимальной производительности и поддержки в различных лесах интегрируйте эту зону с AD DS и настройте каждый полномочный DNS-сервер при помощи локальной копии. Если публикуется расположение зоны GlobalNames посредством записи ресурса Расположение службы (Service Location, SRV), зона предоставляет уникальные однокомпонентные имена по всему лесу. В отличие от WINS, зона GlobalNames предназначена для разрешения однокомпонентных имен для подмножества имен хостов, обычно записей ресурса CNAME для корпоративных серверов. Зона GlobalNames не предназначена для разрешения одноранговых имен, например разрешения имен рабочих станций. Для этого существует LLMNR.

Если зона GlobalNames настроена правильно, разрешение однокомпонентных имен работает следующим образом:

1. К однокомпонентному имени, которое запрашивает клиент, добавляется основной DNS-суффикс клиента. Затем запрос передается DNS-серверу.
2. Если полное имя компьютера не получается разрешить, клиент запрашивает разрешение при помощи списков поиска DNS-суффикса, если они имеются.
3. Если ни один из вариантов имени не удается разрешить, клиент запрашивает разрешение посредством однокомпонентного имени.
4. Если однокомпонентное имя имеется в зоне GlobalNames, имя разрешает DNS-сервер, на котором размещена зона. В противном случае, запрос передастся в WINS.

Зона GlobalNames обеспечивает разрешение однокомпонентных имен только при условии, что все уполномоченные DNS-серверы работают под

управлением Windows Server 2008 R2 и более поздних версий. Впрочем, иные DNS-серверы, которые не являются уполномоченными ни в одной зоне, могут работать под управлением других операционных систем (например, под управлением UNIX). Динамические обновления в зоне GlobalNames не поддерживаются.

Настройка разрешения имен на DNS-клиентах

Лучший способ настроить разрешение имен на DNS-клиентах зависит от конфигурации сети. Если компьютеры используют DHCP, возможно, лучше настроить DNS через параметры на DHCP-сервере. Если компьютеры используют статические IP-адреса или необходимо указать отдельные параметры DNS на отдельных системах, нужно настроить DNS вручную.

Настроить параметры DNS можно на вкладке DNS окна Дополнительные параметры TCP/IP (Advanced TCP/IP Settings). Чтобы открыть это окно, выполните следующие действия:

1. В Центре управления сетями и общим доступом щелкните по ссылке Изменение параметров адаптера. В окне Сетевые подключения щелкните правой кнопкой мыши по нужному подключению и выберите команду Свойства.
2. Дважды щелкните по протоколу, который хотите настроить — TCP/IPv6 или TCP/IPv4.
3. Если используете DHCP и нужно, чтобы адрес DNS-сервера был задан по DHCP, установите переключатель Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically). В противном случае установите переключатель Использовать следующие адреса DNS-серверов (Use The Following DNS Server Addresses), а затем введите адреса основного и дополнительного DNS-серверов в соответствующих полях.
4. Нажмите кнопку Дополнительно, чтобы открыть диалоговое окно Дополнительные параметры TCP/IP. Перейдите на вкладку DNS и настройте необходимые параметры.

– Адреса DNS-серверов, в порядке использования (DNS server addresses, in order of use) — укажите IP-адрес каждого DNS-сервера, который используется для разрешения доменных имен. Чтобы добавить IP-адрес сервера в список, нажмите кнопку Добавить. Нажмите кнопку Удалить, чтобы удалить адрес выделенного сервера из списка. Чтобы изменить выделенную запись, нажмите кнопку Изменить. Если указано несколько серверов DNS, их приоритет определяется очередностью в списке. Если первый сервер не может ответить на запрос о разрешении имени хоста, запрос посылается на следующий DNS-сервер, и т. д.

Чтобы изменить позицию сервера в списке, выделите его и воспользуйтесь кнопками со стрелками вверх и вниз.

- Дописывать основной DNS-суффикс и суффикс подключения (Append primary and connection specific DNS suffixes) — обычно по умолчанию этот переключатель установлен. Включите этот параметр для разрешения неполных имен компьютеров в основном домене. Допустим, происходит обращение к компьютеру Glandolf в родительском домене microsoft.com. Для разрешения имя компьютера будет автоматически дополнено суффиксом DNS — glandolf.microsoft.com. Если в основном домене компьютера с таким именем нет, запрос не выполняется. Основной домен задается на вкладке Имя компьютера (Computer Name) диалогового окна Свойства системы (System Properties).
- Добавлять родительские суффиксы основного DNS-суффикса (Append parent suffixes of the primary DNS suffix) — по умолчанию этот переключатель установлен. Включите его для разрешения неполных имен компьютеров в иерархии родительских/дочерних доменов. В случае неудачного запроса в ближайшем родительском домене, для попытки разрешения запроса используется суффикс родительского домена более высокого уровня. Этот процесс продолжается, пока не будет достигнута вершина иерархии доменов DNS. Допустим, в запросе указано имя компьютера Glandolf в родительском домене dev.microsoft.com. Сначала DNS пытается разрешить имя компьютера glandolf.dev.microsoft.com, а потом, в случае неудачи, пытается разрешить имя glandolf.microsoft.com.
- Дописывать следующие DNS-суффиксы (по порядку) (Append these DNS suffixes (in order)) — установите этот переключатель, чтобы задать использование особых DNS-суффиксов вместо имени родительского домена. Нажмите кнопку Добавить, чтобы добавить суффикс домена в список. Нажмите кнопку Удалить, чтобы удалить выделенный суффикс домена из списка. Для редактирования выделенной записи нажмите кнопку Изменить. Разрешается указать несколько суффиксов домена. Если первый суффикс не позволяет разрешить имя, DNS применяет следующий суффикс из списка. Если первый суффикс не был разрешен, берется следующий суффикс, и т. д. Чтобы изменить очередность суффиксов домена, выберите нужный суффикс и измените его положение кнопками со стрелками вверх и вниз.
- DNS-суффикс подключения (DNS suffix for this connection) — в этом поле задастся DNS-суффикс подключения, переопределяющий DNS-имена, уже настроенные на использование с данным подключением. Обычно имя домена DNS

указывается на вкладке Имя компьютера диалогового окна Свойства системы.

- Зарегистрировать адреса этого подключения в DNS (Register this connection's addresses in DNS) — включите этот параметр, если нужно зарегистрировать все IP-адреса для этого соединения в DNS с FQDN-именами компьютеров. Этот параметр включен по умолчанию.
- Динамические обновления DNS используются в сочетании с DHCP, чтобы позволить клиенту обновить его запись A (адрес узла), если его IP-адрес изменяется и позволяет DHCP-серверу обновить запись PTR (указатель) для клиента на DNS-сервере. Также можно настроить DHCP-серверы, чтобы они обновляли обе записи (A и PTR) от имени клиента. Динамические обновления поддерживаются DNS-серверами BIND 8.2.1 и более поздними версиями, Windows Server 2000, Windows Server 2003 и более поздними версиями Windows Server.
- Использовать DNS-суффикс подключения при регистрации в DNS (Use this connection's DNS suffix in dns registration) — установите этот флажок, если нужно, чтобы все IP-адреса для данного подключения регистрировались в DNS родительского домена.

Установка DNS-серверов

Любую систему Windows Server 2012 можно настроить как DNS-сервер. Доступны четыре типа DNS-серверов.

- Основной сервер, интегрированный с Active Directory — DNS-сервер полностью интегрированный с Active Directory. Все данные DNS хранятся непосредственно в Active Directory.
- Основной сервер — основной DNS-сервер домена с частичной интеграцией с Active Directory. В этом случае основная копия DNS-записей и конфигурация домена хранится в текстовых файлах с расширением dns.
- Вторичный (дополнительный) сервер — резервный DNS-сервер. Хранит копию DNS-записей, полученную с основного сервера и передачи зон для обновлений. Вторичный сервер при запуске получает всю необходимую информацию с DNS-сервера.
- Сервер пересылки (forward-сервер) — сервер, кэширующий DNS-информацию после lookup-запросов и всегда передающий запросы на другие серверы. Сервер пересылки хранит DNS-информацию до обновления, до истечения срока действия или до перезапуска сервера. В отличие от вторичных серверов forward-сервер не запрашивает полную копию файлов база данных зоны. Это означает, что при запуске сервера пересылки его база данных пуста.

Перед настройкой DNS-сервера требуется установить службу DNS-сервер. Затем можно будет настроить сервер для предоставления ним интегрированного, основного, вторичного DNS-сервиса или DNS-сервиса пересылки.

Установка и настройка службы DNS-сервер

Все контроллеры домена могут работать как DNS-серверы, и при установке контроллера домена предлагается установить и настроить DNS в ходе установки контроллера домена. Если администратор согласился на установку DNS, то служба DNS-сервер будет установлена с автоматически заданной стандартной конфигурацией. Переустановка не требуется.
Если настраивается рядовой сервер и служба DNS-сервер еще не установлена, выполните следующие действия:

1. В диспетчере серверов выберите команду меню Управление | Добавить роли и компоненты или щелкните по ссылке Добавить роли и компоненты на панели приветствия. Будет запущен мастер добавления ролей и компонентов. Если мастер отобразит страницу Перед началом работы, прочитайте приветствие и нажмите кнопку Далее.
2. На странице Выбор типа установки по умолчанию выбран переключатель Установка ролей или компонентов. Нажмите кнопку Далее.
3. На странице Выбор целевого сервера можно выбрать, где нужно установить роли и компоненты — на сервере или виртуальном жестком диске. Выберите либо сервер из пула серверов, либо сервер, на котором можно смонтировать виртуальный жесткий диск (VHD). Если роли и компоненты добавляются на VHD, нажмите кнопку Обзор, а затем используйте окно Обзор виртуальных жестких дисков для выбора VHD. Когда будете готовы продолжить, нажмите кнопку Далее. В списке серверов будут только серверы под управлением Windows Server 2012 и добавленные администратором в диспетчере серверов.
4. На странице Выбор ролей сервера выберите роль DNS-сервер. Если нужно установить дополнительные компоненты, от которых зависит данный компонент, будет отображено соответствующее диалоговое окно. Нажмите кнопку Добавить компоненты для закрытия этого окна и установки требуемых компонентов на сервер. Для продолжения нажмите кнопку Далее трижды.
5. Если на сервере, на который устанавливается роль DNS-сервер, нет необходимых двоичных исходных файлов, сервер получит файлы через службу Windows Update (по умолчанию) или из расположения, указанного в групповой политике. Можно также указать альтернативный источник для исходных файлов. Чтобы

сделать это, щелкните по ссылке Указать альтернативный исходный путь (Specify An Alternate Source Path), в появившемся окне укажите альтернативный путь и нажмите кнопку OK. Для сетевых носителей нужно указать UNC-путь, например, \\CorpServer82\WinServer2012\. Для смонтированных образов введите WIM-путь с префиксом WIM и индексом используемого образа, например, WIM:\\CorpServer82\WinServer2-12\install.wim:4.

6. Нажмите кнопку Установить для начала процесса установки. Страница Ход установки позволяет отслеживать процесс инсталляции. Если окно мастера закрыто, нажмите значок Уведомления в консоли Диспетчер серверов, а затем щелкните по ссылке, предназначенной для повторного открытия мастера.
7. Когда мастер закончит установку роли DNS-сервер, страница Ход установки сообщит об этом. Просмотрите подробности установки, чтобы убедиться, что все фазы инсталляции завершены успешно.
8. Начиная с этого момента, служба DNS-сервер должна запускаться автоматически при каждой перезагрузке сервера. Если она не запустится, нужно запустить ее вручную (см. разд. "Запуск и остановка DNS-сервера" далее в этой главе).
9. После установки DNS-сервера можно использовать консоль Диспетчер DNS (DNS Manager) для настройки и управления DNS-сервером. Для вызова консоли Диспетчер DNS (рис. 16.1) выберите команду DNS из меню Средства в диспетчере серверов.
10. Если настраиваемый сервер не отображается в представлении дерева, нужно подключиться к нему. Щелкните правой кнопкой мыши по узлу DNS в представлении дерева и выберите команду Подключение к DNS-серверу (Connect To DNS Server). Теперь выполните одно из действий:
    - для подключения к локальному компьютеру установите переключатель этот компьютер и нажмите кнопку OK;
    - для подключения к удаленному серверу выберите переключатель другой компьютер (The following computer) и введите имя сервера или IP-адрес, а затем нажмите кнопку OK.
11. Запись для DNS-сервера должна появиться в представлении дерева консоли Диспетчер DNS. Щелкните правой кнопкой мыши на записи сервера и выберите команду Настроить DNS-сервер (Configure A DNS Server). Будет запущен мастер настройки DNS-сервера (Configure A DNS Server Wizard). Нажмите кнопку Далее.
12. На странице Выбор действия по настройке (Select Configuration Action) установите переключатель Настроить только корневые

ссылки (Configure root hints only), чтобы указать, что только базовые DNS-структуры должны быть созданы в этот раз

13. Нажмите кнопку Далее. Мастер произведет поиск существующих структур DNS и при необходимости модифицирует их.
14. Нажмите кнопку Готово для завершения процесса.

Если мастер не может настроить корневые ссылки, нужно настроить их вручную или скопировать их с другого сервера. Однако стандартный набор корневых ссылок уже включен в DNS-сервер, и они должны быть добавлены автоматически. Чтобы убедиться в этом, щелкните правой кнопкой мыши по записи DNS-сервера и выберите команду Свойства. В окне Свойства настроенные в данный момент корневые структуры должны быть показаны на вкладке Корневые ссылки (Root Hints).

Настройка основного DNS-сервера

У каждого домена есть основной DNS-сервер. Можно интегрировать этот сервер в Active Directory или оставить его работать в качестве основного сервера. Основные серверы обладают зонами прямого и обратного просмотра. Прямой просмотр служит для разрешения доменных имен в IP-адреса. Обратный просмотр нужен для проверки подлинности DNS-запросов посредством разрешения IP-адресов в доменные имена.

После установки службы DNS-сервер на сервер можно сконфигурировать основной сервер с помощью следующих действий:

1. Запустите консоль Диспетчер DNS. Если необходимый сервер не отображается, подключитесь к нему, как было описано ранее.
2. Запись DNS-сервера должна быть выведена в дереве консоли Диспетчер DNS. Щелкните правой кнопкой мыши на записи сервера и выберите команду Создать новую зону (New Zone). Будет запущен мастер создания новой зоны (New Zone Wizard). Нажмите кнопку Далее.
3. Можно выбрать тип зоны. Если основной сервер настраивается с интеграцией в Active Directory (на контроллере домена), выберите переключатель Основная зона (Primary zone) и убедитесь, что отмечен флажок Сохранять зону в Active Directory (Store the zone in Active Directory). Если интеграция DNS с Active Directory не нужна, выберите переключатель Основная зона и сбросьте флажок Сохранять зону в Active Directory. Нажмите кнопку Далее.
4. Если зона интегрируется с Active Directory, выберите одну из стратегий репликации (в противном случае перейдите к шагу 6).
    1. Для всех DNS-серверов, работающих на контроллерах домена в этом лесу (To all DNS servers running on domain controllers in this forest) — выберите эту стратегию для самой обширной репликации. Помните, что лес Active Directory содержит также

все деревья доменов, использующие данные каталога совместно с текущим доменом.

2. Для всех DNS-серверов, работающих на контроллерах домена в этом домене (To all DNS servers running on domain controllers in this domain) — выберите эту стратегию, если нужно реплицировать DNS-информацию в пределах текущего домена.
3. Для всех контроллеров домена в этом домене (для совместимости с Windows 2000) (To all domain controllers in this domain (for Windows 2000 compatibility)) — выберите эту стратегию, если нужно реплицировать DNS-информацию всем контроллерам домена в текущем домене, что необходимо для совместимости с Windows 2000.

5. Хотя эта стратегия обеспечивает более широкую репликацию DNS-информации внутри домена и обеспечивает совместимость с Windows 2000, не каждый контроллер домена является DNS-сервером (и не нужно настраивать каждый контроллер домена как DNS-сервер).
6. Нажмите кнопку Далее. Выберите переключатель Зона прямого просмотра (Forward Lookup Zone), а затем нажмите кнопку Далее.
7. Введите полное DNS-имя зоны. Имя зона определяет, как сервер или зона вписываются в доменную иерархию DNS. Например, если создается основной сервер для домена microsoft.com, в качестве имени зоны следует ввести microsoft.com. Нажмите кнопку Далее.
8. Если настраивается основная зона, которая не интегрируется с Active Directory, нужно указать имя файла зоны. Имя файла базы данных зоны DNS по умолчанию должно быть уже введено. Оставьте это имя без изменений или введите новое. Нажмите кнопку Далее.
9. Укажите, будут ли разрешены динамические обновления.
   - Разрешить только безопасные динамические обновления (Allow only secure dynamic updates) — когда зона интегрирована с Active Directory, можно использовать списки управления доступом для ограничения круга клиентов, которые могут осуществлять динамические обновления. Когда включена эта опция, только клиенты с авторизированными учетными записями компьютера и одобренными списками управления доступом могут динамически обновлять свои записи ресурсов в DNS.
   - Разрешить любые динамические обновления (Allow both nonsecure and secure dynamic updates) — выберите эту опцию, чтобы разрешить любому клиенту обновлять свои

записи ресурсов в DNS. Клиенты могут быть безопасными и небезопасными.

- Запретить динамические обновления (Do not allow dynamic updates) — отключает динамические обновления DNS. Нужно выбрать эту опцию, только если зона не интегрирована с Active Directory.

10. Нажмите кнопку Далее. А затем нажмите кнопку Готово для завершения этого процесса. Новая зона будет добавлена на сервер, базовые DNS-записи будут созданы автоматически.
11. Один DNS-сервер может предоставлять сервис для нескольких доменов. Если у вас есть несколько родительских доменов, например microsoft.com и msn.com, нужно повторить этот процесс для настройки остальных зон просмотра. Также надо настроить зоны обратного просмотра.
12. Еще необходимо создать дополнительные записи для любых компьютеров, к которым надо открыть доступ из других DNS-доменов, выполнив действия, описанные в разд. "Управление записями DNS" далее в этой главе.

У большинства организаций есть частная и публичная области сети. Публичная область сети — это, как правило, веб-сервер и внешние почтовые серверы. Публичные области сети предприятия не должны разрешать неограниченный доступ. Вместо этого публичные области должны быть настроены как часть сети периметра. (Сети периметра также известны как DMZ, демилитаризованная зона, и как экранированные подсети. Эти области защищены брандмауэром организации, который ограничивает доступ к внешней сети и запрещает доступ к внутренней сети.) В противном случае, публичные области сети должны располагаться в отдельной и защищенной брандмауэром области.

Приватные области сети — те области, в которых располагаются внутренние серверы организации и рабочие станции. В публичных областях сети параметры DNS находятся в публичном интернет-пространстве. Здесь можно использовать DNS-имя .com, .org, .net или любое другое, зарегистрированное у интернет-регистратора, и выделенные IP-адреса.

В приватной области сети DNS-настройки будут в пространстве частной сети. Здесь можно использовать adatum.com в качестве DNS-имени организации и частные IP-адреса.

Настройка дополнительного DNS-сервера

Дополнительные серверы обеспечивают отказоустойчивость DNS-службы сети. Если используется полная интеграция с Active Directory, настраивать дополнительные серверы не нужно. Достаточно запустить службу DNS на нескольких контроллерах домена, и Active Directory будет реплицировать

информацию DNS на все контроллеры. При использовании частичной интеграции следует настроить дополнительные серверы, чтобы уменьшить нагрузку на основной сервер. В небольшой или средней сети можно использовать в качестве дополнительных серверов DNS-серверы интернет-провайдера. Свяжитесь с провайдером, чтобы он настроил дополнительные DNS-службы.

Поскольку дополнительные серверы используют зоны прямого просмотра для большинства типов запросов, зоны обратного просмотра, скорее всего, не понадобятся. Но зоны обратного просмотра нужны основным серверам, поэтому необходимо настроить их, чтобы обеспечить корректное разрешение доменных имен.

Для установки дополнительных серверов с целью повышения отказоустойчивости и балансировки нагрузки выполните следующие действия:

1. Запустите консоль Диспетчер DNS. Если нужного сервера нет в списке, подключитесь к нему, как было описано ранее.
2. Щелкните правой кнопкой мыши на записи сервера, а затем выберите команду Создать новую зону. Будет запущен мастер создания новой зоны. Нажмите кнопку Далее.
3. На странице Тип зоны (Zone Type) выберите переключатель Дополнительная зона (Secondary Zone). Нажмите кнопку Далее.
4. Дополнительные серверы могут использовать как зоны прямого просмотра, так и зоны обратного просмотра. Сначала нужно создать зону прямого просмотра, поэтому выберите переключатель Зона прямого просмотра (Forward Lookup Zone) и нажмите кнопку Далее.
5. Введите DNS-имя зоны и нажмите кнопку Далее.
6. В списке Основные серверы (Master Servers) введите IP-адрес основного сервера зоны и нажмите клавишу <Enter>. Мастер попытается проверить сервер. Если произошла ошибка, убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Если нужно скопировать данные зоны с других серверов на случай недоступности первого сервера, повторите этот шаг.
7. Нажмите кнопку Далее, а затем кнопку Готово. В большой сети, возможно, придется настроить зоны обратного просмотра на дополнительных серверах. Если это так, воспользуйтесь рекомендациями из следующего раздела.

Настройка зон обратного просмотра Прямые просмотры используются для разрешения доменных имен в IP-адреса. Обратные просмотры служат для разрешения IP-адресов в доменные имена. Каждый сегмент сети должен иметь зону обратного просмотра. Например, если есть три подсети — 192.168.10.0, 192.168.11.0 и 192.168.12.0, должны быть и три зоны обратного просмотра.

Стандартное имя зоны обратного просмотра составляется из идентификатора сети, выстроенного в обратном порядке, и суффикса in-addr.arpa. Зоны обратного просмотра из предыдущего примера будут называться 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa и 12.168.192.in-addr.arpa. Записи зон обратного и прямого просмотра должны быть синхронизированы. В случае сбоя синхронизации может произойти сбой проверки подлинности в домене.

Создать зоны обратного просмотра можно с помощью следующих действий:

1. Запустите консоль Диспетчер DNS. Если нужного сервера нет в списке, подключитесь к нему, как было описано ранее.
2. Щелкните правой кнопкой мыши на записи сервера, а затем выберите команду Создать новую зону. Будет запущен мастер создания новой зоны. Нажмите кнопку Далее.
3. Если настраивается основной сервер, интегрированный в Active Directory (контроллер домена), выберите переключатель Основная зона (Primary Zone) и убедитесь, что флажок Сохранять зону в Active Directory (Store the zone in Active Directory) установлен. Если интеграция DNS с Active Directory не нужна, выберите переключатель Основная зона и сбросьте флажок Сохранять зону в Active Directory.
4. Если настраивается зона обратного просмотра для дополнительного сервера, выберите переключатель Дополнительная зона (Secondary Zone) и нажмите кнопку Далее.
5. Если зона интегрируется с Active Directory, выберите одну из следующих стратегий.
   - Для всех DNS-серверов, работающих на контроллерах домена в этом лесу (To all DNS servers running on domain controllers in this forest) — выберите эту стратегию для самой обширной репликации. Помните, что лес Active Directory содержит также все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - Для всех DNS-серверов, работающих на контроллерах домена в этом домене (To all DNS servers running on domain controllers in this domain) — выберите эту стратегию, если нужно реплицировать DNS-информацию в пределах текущего домена.
   - Для всех контроллеров домена в этом домене (для совместимости с Windows 2000) (To all domain controllers in this domain (for Windows 2000 compatibility)) — выберите эту стратегию, если нужно реплицировать DNS-информацию всем контроллерам домена в текущем домене,

что необходимо для совместимости с Windows 2000. Хотя эта стратегия обеспечивает более широкую репликацию DNS-информации внутри домена и совместимость с Windows 2000, не каждый контроллер домена является DNS-сервером (и не нужно настраивать каждый контроллер домена как DNS-сервер).

6. Выберите переключатель Зона обратного просмотра (Reverse Lookup Zone) и нажмите кнопку Далее.
7. Укажите, для каких адресов нужно создать зону обратного просмотра (IPv4 или IPv6) и нажмите кнопку Далее. Выполните одно из следующих действий.
   - Если настраивается зона обратного просмотра для IPv4, введите идентификатор сети для зоны обратного просмотра. Вводимые значения определяют стандартное имя зоны обратного просмотра. Нажмите кнопку Далее.
   - Если есть несколько подсетей в одной сети, например 192.168.10 и 192.168.11, можно ввести только часть сети в качестве имени зоны. Например, в этом случае нужно использовать имя 168.192.in-addr.arpa и разрешить консоли Диспетчер DNS создать необходимые зоны подсетей, когда они понадобятся.
   - Если настраивается зона обратного просмотра для IPv6, введите префикс сети для зоны обратного просмотра. Имена зон автоматически генерируются на основе вводимых значений. В зависимости от введенного префикса можно создать до восьми зон. Нажмите кнопку Далее.
8. Если настраивается основной или дополнительный сервер, не интегрированный в Active Directory, введите имя файла зоны. Имя файла для базы данных зоны DNS должно быть уже введено. Оставьте его неизменным или введите новое имя. Нажмите кнопку Далее.
9. Укажите, будут ли разрешены динамические обновления.
   - Разрешить только безопасные динамические обновления — когда зона интегрирована с Active Directory, можно использовать списки управления доступом для ограничения круга клиентов, которые могут осуществлять динамические обновления. Когда включена эта опция, только клиенты с авторизированными учетными записями компьютера и одобренными списками управления доступом могут динамически обновлять свои записи ресурсов в DNS.
   - Разрешить любые динамические обновления — выберите эту опцию, чтобы разрешить любому клиенту обновлять

свои записи ресурсов в DNS. Клиенты могут быть безопасными и небезопасными.

- Запретить динамические обновления — отключает динамические обновления DNS. Нужно выбрать эту опцию, только если зона не интегрирована с Active Directory.

10. Нажмите кнопку Далее, а затем кнопку Готово для завершения этого процесса. Новая зона будет добавлена на сервер, базовые DNS-записи будут созданы автоматически. После установки зон обратного просмотра необходимо убедиться в правильности обработки делегирования для зоны. Свяжитесь с IT-отделом или интернет-провайдером, чтобы проверить регистрацию зон в родительском домене.

Настройка глобальных имен

Зона GlobalNames — это специальная зона прямого просмотра, которую нужно интегрировать с AD DS. Если все DNS-серверы работают под управлением Windows Server 2008 или более поздних версий, при развертывании зоны GlobalNames создаются статические, глобальные записи с однокомпонентными именами без использования WINS. Это позволяет пользователям получать доступ к хостам по однокомпонентным именам, не прибегая к FQDN-именам. Использовать зону GlobalNames нужно в случаях, если разрешение имен было решено возложить на DNS, полностью отказавшись от WINS, чтобы в перспективе перейти на IPv6. Поскольку для регистрации обновлений в зоне GlobalNames нельзя использовать динамические обновления, настраивать разрешение однокомпонентных имен следует только для основных серверов.

Разместить зону GlobalNames можно с помощью следующих действий:

1. В консоли Диспетчер DNS выберите DNS-сервер, который также является контроллером домена. Если нужного сервера нет в списке, подключитесь к нему, как было описано ранее.
2. Щелкните правой кнопкой мыши на узле Зоны прямого просмотра (Forward Lookup Zones) и выберите команду Создать новую зону. В окне мастера создания новой зоны нажмите кнопку Далее, чтобы по умолчанию создать основную зону, интегрированную с AD DS. На странице Область репликации зоны, интегрированной в Active Directory (Active Directory Zone Replication Scope) задайте репликацию зоны в лесе и нажмите кнопку Далее. На странице Имя зоны (Zone Name) введите имя GlobalNames. Два раза нажмите кнопку Далее и кнопку Готово.
3. На каждом полномочном DNS-сервере леса введите в командной строке с повышенными полномочиями команду dnscmd ServerName /enableglobalnamessupport 1, где ServerName — имя DNS-сервера, содержащего зону GlobalNames. Чтобы указать

локальный компьютер, введите точку (.) вместо имени компьютера, например, dnscmd . /enableglobalnamessupport 1.

4. Для каждого сервера, доступ к которому должны иметь пользователи, в зону GlobalNames добавьте запись CNAME: в консоли Диспетчер DNS щелкните правой кнопкой мыши на узле GlobalNames, выберите команду Создать псевдоним (CNAME) (New Alias (CNAME)) и создайте новую запись ресурса в открывшемся диалоговом окне.

Полномочный DNS-сервер пытается разрешить запросы в следующем порядке, используя: данные локальной зоны, зону GlobalNames, DNS-суффиксы, WINS. Для динамических обновлений полномочный DNS-сервер проверяет зону GlobalNames перед проверкой данных локальной зоны.

Если нужно, чтобы DNS-клиенты из другого леса использовали зону GlobalNames для разрешения имен, необходимо добавить запись ресурса SRV с именем службы _globalnames._ msdcs в DNS-раздел леса. Запись должна указывать FQDN-имя DNS-сервера, содержаще- го зону GlobalNames.

Управление DNS-серверами

Консоль Диспетчер DNS — это утилита, используемая для управления локальным и удаленными DNS-серверами. Как показано на рис. 16.4, главное окно консоли Диспетчер DNS разделено на две панели. Левая панель позволяет получить доступ к DNS-серверам и их зонам. Правая панель показывает подробности для выбранного в данный момент элемента. Можно работать с консолью Диспетчер DNS тремя способами:

- дважды щелкните на элементе на левой панели, чтобы развернуть список файлов для элемента;
- выделите элемент на левой панели, чтобы просмотреть на правой панели сведения о нем, например состояние зоны и доменные записи;
- щелкните на элементе правой кнопкой мыши, чтобы открыть контекстное меню для элемента.

Папки Зоны прямого просмотра (Forward Lookup Zones) и Зоны обратного просмотра (Reverse Lookup Zones) предоставляют доступ к доменам и подсетям, настроенным для использования на данном сервере. Выбирая папки домена или подсети в левой панели, можно управлять DNS-записями для домена или подсети соответственно.

Добавление и удаление серверов для управления

Можно использовать консоль Диспетчер DNS для управления DNS-серверами так:

1. Щелкните правой кнопкой мыши на узле DNS в дереве консоли и выберите команду Подключение к DNS-серверу (Connect To DNS Server).
2. Если подключаетесь к локальному компьютеру, выберите переключатель этот компьютер. В противном случае выберите переключатель другой компьютер, а затем введите IP-адрес или FQDN-имя узла удаленного компьютера, к которому нужно подключиться.
3. Нажмите кнопку OK. Операционная система Windows Server 2012 попытается подключиться к серверу. Если получится, сервер будет добавлен в консоль.

Если сервер отключен от сети или недоступен по другой причине, соединение не удастся. Но все еще можно добавить сервер в консоль, нажав кнопку Да, когда появится запрос, нужно ли добавить недоступный сервер.

В консоли Диспетчер DNS можно удалить сервер, щелкнув на записи сервера правой кнопкой мыши и выбрав команду Удалить. Для подтверждения действия нажмите кнопку Да. Удаление сервера удаляет его только из списка серверов в консоли, оно не удаляет фактически сам сервер.

Запуск и остановка DNS-сервера

Для управления DNS-серверами можно использовать службу DNS-сервер. Управлять службой (запустить, остановить, приостановить, возобновить работу и перезапустить) можно через оснастку Службы, из командной строки и в консоли Диспетчер DNS. Щелкните правой кнопкой мыши на сервер и выберите команду Все задачи (All Tasks), а далее — нужную команду: Запустить (Start), Остановить (Stop), Приостановить (Pause), Продолжить (Resume) или Перезапустить (Restart).

В диспетчере серверов тоже можно управлять DNS-сервером: разверните узел DNS, щелкните правой кнопкой мыши на сервере, а затем в контекстном меню выберите нужную команду (Запустить службы, Остановить службы и т. д.).

Использование DNSSEC и подпись зон

Операционная система Windows 7 и более поздние версии, так же как и Windows Server 2008 R2 и более поздние версии, поддерживают DNSSEC (DNS Security Extensions, расширения безопасности DNS). Расширения безопасности DNSSEC определены в нескольких рекомендациях RFC: 4033, 4034 и 4035. Эти RFC добавляют проверку подлинности, целостность данных и отказ в доступе к DNS. DNSSEC добавляет следующие записи ресурсов:

- DNSKEY (Domain Name System Key);

- RRSIG (Resource Record Signature);
- NSEC (NextSECure);
- DS (Domain Services).

DNS-клиент, запущенный на этих операционных системах, может отправлять запросы для определения поддержки DNSSEC, которые позволяют DNS-серверам безопасно подписывать зоны, размещать подписанные DNSSEC зоны, обрабатывать соответствующие записи и осуществлять проверку подлинности и аутентификацию. Способ работы DNS-клиента с DNSSEC определяется в таблице политик разрешения имен (Name Resolution Policy Table, NRPT), которая содержит настройки, определяющие поведение DNS-клиента. Обычно таблицей NRPT нужно управлять через групповую политику.

Когда DNS-сервер, размещающий подписанную зону, получает запрос, сервер возвращает цифровые подписи вместе с запрошенными клиентом записями. Распознаватель или другой сервер, настроенный на проверку подписи, могут получить открытый ключ пары "открытый/закрытый ключи" и установить, что ответ является подлинным.

В качестве части плана предразвертывания нужно идентифицировать DNS-зоны, которые будут защищены цифровыми подписями. DNS-сервер для Windows Server 2012 обладает следующими расширениями для DNSSEC.

 Поддержка динамических обновлений в зонах, интегрированных в Active Directory. Ранее, если зона домена Active Directory была подписана, нужно было вручную обновлять все SRV-записи и другие ресурсные записи. Теперь в этом нет необходимости, поскольку DNS-сервер делает это автоматически.

- Поддержка онлайн-подписей, автоматического управления ключами, автоматического распределения якорей доверия (trust anchors). Ранее нужно было настраивать и управлять подписями, ключами и якорями. Теперь в этом нет необходимости, поскольку DNS-сервер делает это автоматически.
- Поддержка проверки записей, подписанных с обновленными стандартами DNSSEC (стандарты NSEC3 и RSA/SHA-2). Ранее записи подписывались с помощью стандартов NSEC3 и RSA/SHA-2.

Также помните о следующем.

- Для зон, не интегрированных с Active Directory, основной и все дополнительные серверы, размещающие зону, должны работать под управлением Windows Server 2008 R2 или более поздней версии или под управлением другой операционной системой, где есть DNSSEC-совместимый DNS-сервер.
- Для зон, интегрированных с Active Directory, каждый контроллер домена, который является DNS-сервером в домене, должен работать под управлением Windows Server 2008 R2 или более

поздней версии, если подписанная зона настроена для репликации всем DNS-серверам в домене. Каждый контроллер домена, который действует как DNS-сервер в лесу, должен работать под управлением Windows Server 2008 R2 или более поздней версии, если подписанная зона реплицируется всем DNS-серверам леса.

- Для смешанного окружения все серверы, являющиеся авторитетными (заслуживающими доверия), для DNSSEC-подписанной зоны должны поддерживать DNSSEC. DNS-клиенты с поддержкой DNSSEC, запрашивающие DNSSEC-данные и проверку подлинности, должны быть настроены на использование DNS-запросов серверу с поддержкой DNSSEC. Серверы с поддержкой DNSSEC должны быть настроены так, чтобы они отправляли рекурсивные запросы серверам без поддержки DNSSEC.

Защита DNS-зон с помощью цифровых подписей — это многоэтапный процесс. Как часть этого процесса, нужно назначить мастер ключей (key master).

Любой авторитетный сервер, содержащий основную копию зоны, может выступать в роли такого сервера. Далее нужно сгенерировать ключ для подписи ключа (Key Signing Key, KSK) и ключ для подписи зоны (Zone Signing Key, ZSK). Ключ для подписи ключа — аутентификационный ключ, имеющий закрытый и открытый ключи, связанные с ними. Закрытый ключ (private key) служит для подписи всех записей DNSKEY в корне зоны. Открытый ключ (public key) используется как якорь доверия для проверки DNS-ответов. Ключ для подписи зоны применяется для подписей записей зоны.

После того как ключи будут сгенерированы, необходимо создать записи для отрицания существования при проверке подлинности с использованием более безопасного стандарта NSEC3 или менее безопасного стандарта NSEC. Поскольку якоря доверия используются для проверки DNS-ответов, также нужно указать, как якоря доверия будут обновляться и распространяться. Обычно нужно автоматически обновлять и распространять якоря доверия.

По умолчанию записи подписываются с помощью шифрования SHA-1 и SHA-256. При желании можно выбрать другие алгоритмы шифрования.

Не нужно производить процесс настройки при каждой подписи зоны. Ключи и другие параметры подписи можно использовать повторно.

Чтобы подписать зону, выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на зоне, которую нужно подписать. Из контекстного меню выберите команду DNSSEC | Подписать зону (Sign The Zone). Будет запущен мастер подписывания зоны (Zone Signing Wizard). Прочитайте приветствие и нажмите кнопку Далее.

2. На странице Параметры подписывания (Signing Options) выберите переключатель Настроить параметры подписывания зоны (Customize zone signing parameters) и нажмите кнопку Далее.
3. Выберите мастер ключей для зоны. Любой сервер, заслуживающий доверия, который содержит основную копию зоны, может действовать в роли мастера ключей. Когда будете готовы продолжить, нажмите кнопку Далее дважды.
4. На странице Ключ подписывания ключа (KSK) (Key Signing Key) настройте KSK-ключ. Нажмите кнопку Добавить, примите или измените параметры по умолчанию и нажмите кнопку OK. Как только будете готовы, нажмите кнопку Далее дважды.
5. На странице Ключ подписывания зоны (Zone Signing Key) настройте ZSK-ключ. Нажмите кнопку Добавить, примите или измените параметры по умолчанию, а затем нажмите кнопку OK. Когда будете готовы, нажмите кнопку Далее пять раз.
6. Когда мастер подпишет зону, нажмите кнопку Готово.

Чтобы подписать зону с использованием существующих параметров подписи, выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на зоне, которую нужно подписать. Из контекстного меню выберите команду DNSSEC | Подписать зону. Будет запущен мастер подписывания зоны. Прочитайте приветствие и нажмите кнопку Далее.
2. На странице Параметры подписывания выберите переключатель Подписать зону с использованием параметров существующей зоны (Sign the zone with parameters of an existing zone). Введите имя существующей подписанной зоны, например cpandl.com, и нажмите кнопку Далее.
3. На странице Мастер ключей (Key Master) выберите мастер ключей для зоны. Любой сервер, заслуживающий доверия, который содержит основную копию зоны, может действовать в роли мастера ключей. Как только будете готовы продолжить, нажмите кнопку Далее дважды.
4. После того как мастер подпишет зону, нажмите кнопку Готово.

Создание дочерних доменов в зонах

Используя консоль Диспетчер DNS, можно создать дочерние домены в зоне. Например, если создана основная зона microsoft.com, можно создать поддомены hr.microsoft.com и mis.microsoft.com. Создать дочерние домены можно так:

1. В консоли Диспетчер DNS разверните папку Зоны прямого просмотра для сервера, с которым нужно работать.

2. Щелкните правой кнопкой мыши на записи родительского домена и выберите команду Создать домен (New Domain).
3. Введите имя нового домена и нажмите кнопку OK. Для hr.microsoft.com нужно просто ввести hr. Для mis.microsoft.com нужно ввести mis.

Создание дочерних доменов в отдельных зонах

По мере роста организации иногда нужно разделить пространство имен DNS на отдельные зоны. Штаб-квартира корпорации может находиться в зоне родительского домена microsoft.com. Филиалы могут иметь зону для каждого офиса, например memphis. microsoft.com, newyork.microsoft.com и la.microsoft.com.

Создать дочерние домены в разных зонах можно так:

1. В каждом дочернем домене установите DNS-сервер и создайте необходимые зоны прямого и обратного просмотра для дочернего домена, как было описано ранее в разд. "Установка DNS-серверов".
2. Делегируйте полномочия для каждого дочернего домена на полномочном DNS-сервере родительского домена. Делегирование полномочий позволяет дочернему домену разрешать и отвечать на DNS-запросы компьютеров, находящихся внутри и за пределами локальной подсети.

Чтобы делегировать полномочия дочернему домену, выполните следующие действия:

1. В консоли Диспетчер DNS раскройте папку Зоны прямого просмотра нужного сервера.
2. Щелкните правой кнопкой мыши по родительскому домену и выберите команду Создать делегирование (New Delegation). Запустится мастер делегирования (New Delegation Wizard). Нажмите кнопку Далее.
3. Введите имя делегированного домена, например service, а затем нажмите кнопку Далее. Введенное имя будет отражено в поле Полное доменное имя (FQDN) (Fully qualified domain name (FQDN)).
4. Нажмите кнопку Добавить. Откроется окно Новая запись сервера имен (New Name Server Record).
5. В поле Полное доменное имя сервера (Server fully qualified domain name) ведите полное имя DNS-сервера для дочернего домена, например corpserver01.memphis.adatum.com, а затем нажмите кнопку Разрешить в адрес (Resolve). Сервер отправит запрос и добавит разрешенный IP-адрес сервера в список IP-адреса записи сервера имен (Name Servers).

6. Повторите шаг 5, чтобы добавить дополнительные серверы имен. Порядок записей определяет, какой из IP-адресов будет использован первым. При необходимости измените порядок с помощью кнопок Вверх (Up) и Вниз (Down). Нажмите кнопку OK, чтобы закрыть диалоговое окно Новая запись сервера имен.
7. Нажмите кнопку Далее, а затем кнопку Готово.

Удаление домена или подсети

Удаление домена или подсети удаляет ее без возможности восстановления с DNS-сервера. Для удаления домена или подсети выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на записи домена или подсети.
2. Из контекстного меню выберите команду Удалить и подтвердите удаление, нажав кнопку Да.
3. Если домен (или подсеть) интегрирован с Active Directory, будет отображено предупреждение. Нажмите кнопку Да, чтобы подтвердить удаление DNS-информации из Active Directory.

Удаление домена или подсети удаляет все DNS-записи в файле зоны, но не удаляет файлы зоны с основного или дополнительного сервера, который не интегрирован с Active Directory. Фактически файл зоны останется в каталоге %SystemRoot%\System32\Dns. Можно удалить этот файл после удаления зоны из консоли Диспетчер DNS.

Управление записями DNS

После создания необходимых файлов зоны можно добавить в них записи. Для компьютеров, к которым необходим доступ из Active Directory и доменов DNS, нужно создать записи DNS. Хотя существует много типов записей DNS, большинство из них не используется часто. Давайте сконцентрируем внимание на тех записях, которые чаще всего востребованы.

- A (IPv4-адрес) — используется для преобразования имени узла в IPv4-адрес. Когда у компьютера есть несколько сетевых карт, IPv4-адресов (или несколько и сетевых карт, и адресов) для компьютера должно быть создано несколько записей адреса.
- AAAA (IPv6-адрес) — используется для преобразования имени узла в IPv6-адрес. Когда у компьютера несколько сетевых карт, IPv6-адресов (или несколько и сетевых карт, и адресов), для компьютера должно быть создано несколько записей адреса.
- CNAME (canonical name, каноническое имя) — устанавливает псевдоним для имени узла. Например, можно с помощью этой записи установить псевдоним www.microsoft.com для узла zeta.microsoft.com.

- MX (mail exhanger) — указывает сервер обмена почты для домена, позволяющий отправлять сообщения электронной почты корректным почтовым серверам в домене.
- NS (name server) — определяет сервер имен для домена. У каждого основного и дополнительного сервера должна быть эта запись.
- PTR (указатель) — создает указатель, преобразующий IP-адрес в имя узла (обратный запрос).
- SOA (start of authority, начало полномочий) — объявляет хост, обладающий наибольшими полномочиями в зоне и потому являющийся наилучшим источником DNS-информации в зоне. Начальная запись зоны (SOA) должна быть в каждом файле зоны (который создается автоматически при добавлении зоны). Также она объявляет другую информацию о зоне, например, ответственное лицо, интервал обновления, интервал повтора и т. д.

Добавление записей адреса и указателя

Записи типов A и AAAA используются для преобразования имен узла в IP-адреса. Запись PTR служит для обратного запроса, т. е. для преобразования IP-адреса в имя узла. Можно создать записи адреса и указателя одновременно или по отдельности.

Чтобы создать новый элемент узла при помощи записей адреса и указателя, выполните следующие действия:

1. В консоли Диспетчер DNS раскройте папку Зоны прямого просмотра нужного сервера.
2. Щелкните правой кнопкой мыши на домене, который нужно обновить, и выберите команду Создать узел (A или AAAA) (New Host (A Or AAAA)).
3. Введите имя компьютера, например servicespc85, и IP-адрес, например 192.168.10.58.
4. Установите флажок Создать соответствующую PTR-запись (Create associated pointer (PTR) record). Можно создать PTR-записи, только если соответствующая зона обратного просмотра доступна. Создать этот файл можно, следуя рекомендациям из разд. "Настройка зон обратного просмотра" ранее в этой главе. Опция Разрешать любому прошедшему проверку пользователю... (Allow Any Authenticated User) доступна, только когда DNS-сервер настроен на контроллере домена.
5. 5. Нажмите кнопку Добавить узел (Add Host), а затем кнопку OK. Повторите этот процесс для добавления других узлов.
6. 6. Нажмите кнопку Готово, когда закончите.

Добавление записи указателя позже

Чтобы позже добавить PTR-запись для узла, выполните следующие действия:

1. В консоли Диспетчер DNS раскройте папку Зоны обратного просмотра нужного сервера.
2. Щелкните правой кнопкой мыши на подсети, которую нужно обновить, и выберите команду Создать указатель (New Pointer (PTR)).
3. Введите IP-адрес узла, например 192.168.1.95, и имя узла, например servicespc54. Нажмите кнопку OK.

Добавление DNS-псевдонимов с помощью CNAME

Псевдонимы узлов определяются посредством записи CNAME. Псевдонимы позволяют одному узлу выдавать себя за несколько узлов. Например, узел gamma.microsoft.com может быть как узлом www.microsoft.com, так и ftp.microsoft.com.

Для создания записи CNAME выполните следующие действия:

1. В консоли Диспетчер DNS разверните папку Зоны прямого просмотра нужного сервера.
2. Щелкните правой кнопкой мыши на домене, который нужно обновить, и выберите команду Создать псевдоним (CNAME) (New alias (CNAME)).
3. В поле Псевдоним (Alias Name) введите псевдоним. Псевдоним — это однокомпонентное имя, например www или ftp.
4. В поле Полное доменное имя (FQDN) конечного узла (Fully qualified domain name (FQDN) for target host) введите полное имя компьютера, для которого создается псевдоним.
5. Нажмите кнопку OK.

Добавление почтовых серверов

Записи MX используются для идентификации серверов обмена почтовыми сообщениями домена, которые отвечают за обработку или пересылку почты внутри домена. Создавая MX-запись, нужно указать номер предпочтения почтового сервера — число от 0 до 65 535, определяющее приоритет почтового сервера в домене. Почтовый сервер с наименьшим предпочтением обладает наибольшим приоритетом и получает почту в первую очередь. В случае сбоя доставки почты используется следующий предпочитаемый номер по возрастанию.

Для создания MX-записи выполните следующие действия:

1. В консоли Диспетчер DNS разверните папку Зоны прямого просмотра нужного сервера.
2. Щелкните правой кнопкой мыши на домене, который нужно обновить, и выберите команду Создать почтовый обменник (MX) (New Mail Exchanger (MX)).

3. Теперь можно создать запись почтового сервера, заполнив следующие поля.
   - Узел или дочерний домен (Host or child domain) — при желании введите однокомпонентное имя почтового сервера. В большинстве случаев можно оставить это поле незаполненным, и таким образом имя почтового сервера будет совпадать с именем родительского домена.
   - Полное доменное имя (FQDN) (Fully qualified domain name (FQDN)) — введите FQDN-имя домена, к которому относится запись почтового сервера, например cpandl.com.
   - Полное доменное имя (FQDN) почтового сервера (Fully qualified domain name (FQDN) of mail server) — введите FQDN-имя почтового сервера, например corpmail.cpand.com. Сообщения для ранее указанного домена передаются на этот сервер с целью доставки.
   - Приоритет почтового сервера (Mail Server Priority) — введите номер предпочтения для узла от 0 до 65 535.
   - Назначайте номера предпочтения, оставляя возможность для роста. Например, используйте 10 для сервера с наивысшим приоритетом, 20 — для следующего сервера, 30 — еще для одного сервера.
   - Нельзя вводить многокомпонентное имя в поле Узел или дочерний домен. Если нужно ввести многокомпонентное имя, будет создана MX-запись с неправильным уровнем DNS-иерархии. Создайте дополнительный уровень домена, а затем добавьте MX-запись на этом уровне.
4. Нажмите кнопку OK.

Добавление серверов имен

Записи NS указывают серверы имен для домена. Каждый основной и дополнительный серверы имен должны быть объявлены с помощью этой записи. Если дополнительные службы имен предоставляет интернет-провайдер, убедитесь, что вставили соответствующие NS-записи.

Создать NS-запись можно так:

1. В консоли Диспетчер DNS разверните папку Зоны прямого просмотра нужного сервера.
2. Отобразите DNS-записи домена, развернув его узел в дереве консоли.
3. Щелкните правой кнопкой мыши на существующей NS-записи в области просмотра и выберите команду Свойства. Диалоговое окно свойств домена откроется на вкладке Серверы имен (Name Servers).

4. Нажмите кнопку Добавить. Откроется диалоговое окно Новая запись сервера имен (New Name Server Record).
5. В поле Полное доменное имя (FQDN) сервера (Server fully qualified domain name (FQDN)) введите полное хост-имя DNS-сервера дочернего домена, например corpserver01.cpandl.com. Нажмите кнопку Разрешить в адрес (Resolve). Сервер разрешит имя и добавит разрешенный IP-адрес в список IP-адреса записи сервера имен (Name Servers).
6. Повторите шаг 5, чтобы определить дополнительные серверы имен. Порядок записей определяет, какой из IP-адресов будет использован первым. При необходимости измените порядок с помощью кнопок Вверх и Вниз. Нажмите кнопку OK, чтобы закрыть диалоговое окно Новая запись сервера имен.
7. Нажмите кнопку OK, чтобы сохранить изменения.

Просмотр и обновление DNS-записей

Чтобы просмотреть или обновить DNS-записи, выполните следующие действия:

1. Дважды щелкните на зоне, с которой нужно работать. На правой панели будут отображены записи зоны.
2. Дважды щелкните на записи DNS, которую нужно просмотреть или обновить. Откроется окно Свойства. Внесите необходимые изменения и нажмите кнопку OK.

Обновление свойств зоны и записи SOA

У каждой зоны есть свои отдельные свойства, которые можно настроить. Эти свойства устанавливают общие параметры зоны посредством записи SOA, уведомления об изменении и WINS-интеграции.

В консоли Диспетчер DNS можно установить свойства зоны одним из двух способов:

- щелкните правой кнопкой мыши на зоне, которую нужно обновить, и выберите команду Свойства;
- выберите зону, а затем выберите команду Свойства из меню Действия. Окна Свойства для зон прямого и обратного просмотра идентичны за исключением вкладок WINS и WINS-R. В зонах прямого просмотра используется вкладка WINS для настройки просмотров NetBIOS-имен компьютеров. В зонах обратного просмотра используется вкладка WINS-R для настройки обратного просмотра для NetBIOS-имен компьютера.

Изменение записи SOA

Начальная запись SOA объявляет полномочный сервер имен зоны и устанавливает общие свойства зоны, например интервалы повторов и обновлений. Можно изменить эту информацию так:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на зоне, которую нужно обновить, и выберите команду Свойства.
2. Перейдите на вкладку Начальная запись зоны (SOA) (Start of Authority (SOA)) и обновите текстовые поля.

На вкладке Начальная запись зоны (SOA) доступны следующие параметры.

- Серийный номер (Serial number) — отражает версию файлов базы данных DNS. Номер обновляется автоматически при внесении изменений в файлы зоны, но можно обновить его и вручную. По этому номеру дополнительные серверы определяют, изменилась ли зона. Если серийный номер основного сервера превышает серийный номер дополнительного сервера, записи изменились, и дополнительный сервер может запросить DNS-записи зоны. Кроме того, можно настроить DNS на уведомление дополнительных серверов об изменениях (что ускоряет процесс обновления).
- Основной сервер (Primary server) — полное доменное имя сервера, в конце которого стоит точка. Она обозначает конец имени и гарантирует, что к записи не будет добавлена информация о домене.
- Ответственное лицо (Responsible person) — адрес электронной почты лица, ответственного за домен. По умолчанию здесь стоит имя hostmaster, за которым следует точка. Это обозначает адрес hostmaster@домен.com. При вводе здесь другого адреса замените точкой символ @ в адресе электронной почты и в конце адреса также поставьте точку.
- Интервал обновления (Refresh interval) — интервал, через который дополнительный сервер проводит проверку обновлений зоны. Если интервал установлен в 60 минут, изменения на дополнительном сервере отобразятся через час. Можно уменьшить сетевой трафик, увеличивая это значение.
- Интервал повтора (Retry interval) — время после сбоя, в течение которого дополнительный сервер не загружает базы данных зоны. Если задан интервал 10 минут, после сбоя передачи базы данных зоны дополнительный сервер ждет 10 минут, прежде чем отправить новый запрос.
- Срок жизни истекает после (Expires after) — период времени, в течение которого информация зоны на дополнительном сервере

считается достоверной. Если дополнительный сервер в течение этого времени не может загрузить данные с основного сервера, данные в кэше дополнительного сервера устаревают, и дополнительный сервер перестает отвечать на DNS-запросы. Установка этого параметра в 7 дней позволяет данным на дополнительном сервере быть достоверными неделю.

- Мин. срок жизни TTL (по умолчанию) (Minimum (default) TTL) — минимальное время жизни записей на дополнительном сервере. Данное значение можно установить в днях, часах, минутах или секундах. Когда это время заканчивается, дополнительный сервер считает срок действия соответствующей записи истекшим и сбрасывает ее. После этого необходимо отправлять очередной запрос на основной сервер. Делайте минимальный срок жизни относительно большим, например 24 часа. Это сократит сетевой трафик и повысит производительность. С другой стороны, нужно помнить, что высокое значение замедляет распространение обновлений через Интернет.
- Срок жизни (TTL) записи (TTL for this record) — время жизни конкретной SOA-записи в формате ДД:ЧЧ:ММ:СС. Как правило, оно должно совпадать с минимальным временем жизни всех записей.

Разрешение и запрещение передачи зоны

При передаче зоны отправляется копия информации зоны другим DNS-серверам. Эти серверы могут находиться в одном и том же домене или в разных доменах. По соображениям безопасности в Windows Server 2012 передача зоны отключена. Чтобы включить эту функцию для дополнительных серверов организации или для DNS-серверов интернет-провайдера, нужно разрешить передачу зоны и указать типы серверов, на которые разрешено передавать зону.

Хотя можно разрешить передачу зоны любому серверу, это открывает потенциальные проблемы с безопасностью. Вместо этого нужно ограничить доступ к информации зоны так, чтобы запрашивать обновления с основного сервера зоны могли только указанные вами серверы. Это позволит ограничить запросы определенной группой дополнительных серверов, например серверов имен поставщика Интернета, а также скрыть внутреннюю сеть от внешнего мира.

Чтобы разрешить передачи зоны и ограничить доступ к базе данных основной зоны, выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на домене или подсети, которые хотите обновить, и выберите команду Свойства.
2. Перейдите на вкладку Передачи зон (Zone Transfers).

3. Чтобы ограничить переносы серверами имен, перечисленными на вкладке Серверы имен (Name Servers), установите флажок Разрешить передачи зон (Allow zone transfers) и установите переключатель только на серверы, перечисленные на странице серверов имен (Only to servers listed on the Name Servers tab).
4. Чтобы ограничить переносы указанными серверами, установите флажок Разрешить передачи зон и выберите переключатель только на серверы из этого списка (Only to the following servers). Затем нажмите кнопку Изменить, чтобы открыть диалоговое окно Разрешить передачи зон (Allow Zone Transfers). Щелкните на колонке IP-адрес (IP Address), введите IP-адрес дополнительного сервера зоны и нажмите клавишу <Enter>. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Если необходимо копировать данные зоны из других серверов на случай недоступности первого сервера, добавьте IP-адреса и других серверов. Нажмите кнопку OK.
5. Нажмите кнопку OK, чтобы сохранить изменения.

Уведомление дополнительных серверов об изменениях

Свойства зоны устанавливаются посредством SOA-записи. Параметры зоны регулируют распространение информации DNS по сети. Можно также указать основному серверу, чтобы он рассылал уведомления дополнительным серверам имен при наличии изменений в базе данных зоны. Для этого выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на домене или подсети, которые нужно обновить, и выберите команду Свойства.
2. На вкладке Передачи зон нажмите кнопку Уведомить (Notify). Откроется окно. Используйте окно Уведомление, чтобы уведомить все дополнительные серверы, указанные либо на вкладке Серверы имен, или в списке этого окна
3. Чтобы уведомлять серверы имен, перечисленные на вкладке Серверы имен, установите флажок Автоматически уведомлять (Automatically notify) и переключатель Уведомлять серверы со страницы серверов имен (Servers listed on the Name Servers tab).
4. Чтобы указать серверы для получения уведомлений, установите флажок Автоматически уведомлять и переключатель Только указанные серверы (The following servers). Щелкните в списке на IP-адресе, введите IP-адрес дополнительного сервера зоны и нажмите клавишу <Enter>. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и введен

правильный IP-адрес. Если нужно уведомлять другие серверы, добавьте их IP-адреса.
5. Дважды нажмите кнопку OK.

Установка типа зоны

При создании зоны назначаются тип зоны и режим интеграции с Active Directory. Можно изменить тип и режим интеграции в любое время с помощью следующих действий:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на домене или подсети, которые нужно обновить, и выберите команду Свойства.
2. На вкладке Общие напротив параметра Тип нажмите кнопку Изменить. В окне Изменение типа зоны (Change Zone Type) выберите новый тип зоны.
3. Для интегрирования зоны с Active Directory установите параметр Хранить зону в Active Directory (Store the zone in Active Directory).
4. Чтобы удалить зону с Active Directory, выключите параметр Хранить зону в Active Directory (Store the zone in Active Directory).
5. Дважды нажмите кнопку OK.

Включение и выключение динамических обновлений

Динамические обновления позволяют DNS-клиентам регистрировать и обслуживать свои записи адреса и указателя. Это полезно для компьютеров, которые динамически настраиваются средствами DHCP. Включение динамических обновлений поможет динамически настроенным компьютерам определить положение друг друга в сети. Если зона интегрирована в Active Directory, есть возможность включить запрос на безопасные обновления. При безопасных обновлениях определение компьютеров и пользователей, которым позволено динамически обновлять DNS, происходит при помощи списков управления доступом.

Можно включить и отключить динамические обновления с помощью следующих действий:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на домене или подсети, которые нужно обновить, и из контекстного меню выберите команду Свойства.
2. Используйте список Динамическое обновление (Dynamic Updates) на вкладке Общие, чтобы включить или выключить динамические обновления:
   - Никакие (None) — отключает динамические обновления;
   - Небезопасные и безопасные (Nonsecure and Secure) — включает небезопасные и безопасные динамические обновления;

- Только безопасные (Secure Only) — включает только безопасные инамические обновления. Этот вариант доступен лишь при интеграции с Active Directory.

3. Нажмите кнопку OK.

Параметры интеграции DNS также должны быть настроены для DHCP. Подробно речь об интеграции DHCP и DNS шла в главе 15.

Управление конфигурацией DNS-сервера и безопасностью

Окно Свойства сервера (Server Properties) используется для управления основной конфигурацией DNS-серверов. С его помощью можно включать и отключать IP-адреса для сервера и контролировать доступ к серверам за пределами организации. Также можно настроить параметры наблюдения, журналирования и другие расширенные параметры.

Включение и отключение IP-адресов для DNS-сервера

По умолчанию многодомные DNS-серверы отвечают на DNS-запросы по всем доступным сетевым интерфейсам и IP-адресам, настроенным для использования. С помощью консоли Диспетчер DNS можно заставить сервер отвечать на запросы только с заданных IP-адресов. Нужно убедиться, что у сервера есть как минимум один IPv4-интерфейс и один IPv6-интерфейс.

Чтобы указать, какие IP-адреса будут использоваться для ответа на запросы, выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду Свойства.
2. На вкладке Интерфейсы (Interfaces) выберите переключатель только по указанным IP-адресам (Only the following IP addresses). Выберите IP-адреса, по которым сервер должен отвечать на DNS-запросы. Только выбранные IP-адреса будут использоваться для DNS. Все другие IP-адреса на сервере будут недоступны для DNS.
3. Нажмите кнопку OK.

Управление доступом к внешним DNS-серверам

Ограничение доступа к информации зоны позволяет указать, какие внутренние и внешние серверы могут получать доступ к основному серверу. Для внешних серверов это означает управление возможностью подключения из внешнего мира. Также можно задать, какие DNS-серверы организации могут получать доступ к серверам за ее пределами. Для этого следует настроить внутри домена DNS-пересылку.

С точки зрения пересылки серверы DNS в домене можно настроить одним из следующих образов.

- Серверы без пересылки (Nonforwarders) — серверы должны передавать DNS-запросы, которые они не смогли разрешить, на заданные серверы пересылки. В целом, эти серверы выступают в роли DNS-акцептов для серверов пересылки.
- Только пересылка (Forwarding-only) — серверы способны только кэшировать ответы и передавать запросы на серверы пересылки. Известны также как кэширующие DNS-серверы.
- Серверы пересылки (Forwarders Servers) — серверы, получающие запросы от серверов без пересылки или только с пересылкой. Для разрешения запросов серверы пересылки используют нормальные способы коммуникаций DNS.
- Серверы условной пересылки (Conditional forwarders) — серверы, перенаправляющие запросы на основе домена DNS. Условное перенаправление удобно, когда в организации есть несколько внутренних доменов.

Нельзя настроить корневой сервер домена для пересылки (за исключением условной пересылки, используемой с внутренним разрешением имен). Все остальные серверы можно настроить для пересылки.

Создание серверов без пересылки и кэширующих серверов

Для создания серверов без пересылки или кэширующих серверов выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду Свойства.
2. Перейдите на вкладку Дополнительно. Чтобы настроить сервер в качестве сервера без пересылки, убедитесь, что сброшен флажок Отключить рекурсию (и серверы пересылки) (Disable recursion), нажмите кнопку OK и пропустите следующие действия. Чтобы настроить сервер как сервер пересылки (кэширующий сервер), убедитесь, что установлен флажок Отключить рекурсию (и серверы пересылки).
3. На вкладке Сервер пересылки (Forwarders) нажмите кнопку Изменить. Откроется окно Редактировать серверы пересылки (Edit Forwarders).
4. Щелкните по колонке IP-адрес, введите IP-адрес сервера пересылки сети и нажмите клавишу <Enter>. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и введен правильный IP-адрес. Повторите процесс, чтобы задать IP-адреса других серверов пересылки.
5. Установите значение поля Время ожидания пересылки (Forward queries time out). Это значение задает время, в течение которого сервер без пересылки повторяет попытки опросить текущий сервер пересылки при отсутствии ответа. По истечении времени

ожидания сервер без пересылки пытается запросить следующий сервер пересылок из списка. По умолчанию время ожидания равно 3 секундам. Нажмите кнопку OK.

Создание серверов пересылки

Выступать в роли сервера пересылок способен любой DNS-сервер, если он не настроен в качестве сервера без пересылок или кэширующего сервера. На серверах пересылки в сети убедитесь в том, что флажок Отключить рекурсию сброшен и сервер не настроен на перенаправление запросов на другие DNS-серверы в домене.

Настройка сервера условной пересылки

Если есть несколько внутренних доменов, нужно задуматься о настройке условной пересылки, которая позволяет направлять запросы конкретных доменов для разрешения на конкретные DNS-серверы. Условная пересылка полезна, если в организации есть несколько внутренних доменов и нужно разрешать запросы между ними.

Для настройки условной пересылки выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на папке Серверы условной пересылки (Conditional Forwarders) нужного сервера. В контекстном меню выберите команду Создать сервер условной пересылки (New Conditional Forwarder).
2. В диалоговом окне Создать сервер условной пересылки (New Conditional Forwarder) введите имя домена, в который следует пересылать запросы, например adatum.com.
3. Щелкните по колонке IP-адрес, введите IP-адрес полномочного DNS-сервера в указанном домене и нажмите клавишу <Enter>. Повторите процесс, чтобы указать дополнительные IP-адреса.
4. При использовании интеграции DNS с Active Directory установите флажок Сохранять условный сервер пересылки в Active Directory и реплицировать ее следующим образом (Store this conditional forwarder in Active Directory) и выберите одну из следующих стратегий репликации.
   - Все DNS-серверы в этом лесу (All DNS servers in this forest) — самая широкая стратегия репликации. Лес Active Directory включает все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - Все DNS-серверы в этом домене (All DNS servers in this domain) — выберите эту стратегию, чтобы реплицировать информацию DNS внутри текущего домена и его дочерних доменов.
   - Все контроллеры домена в этом домене (для совместимости с ОС Windows 2000) (All domain controllers in this domain) —

выберите эту стратегию, если хотите реплицировать информацию DNS на все контроллеры домена внутри текущего домена и его дочерних доменов. Хотя эта стратегия обеспечивает более широкую репликацию информации DNS внутри домена, не каждый контроллер домена является DNS-сервером (и не нужно настраивать каждый контроллер домена как DNS-сервер).

5. Установите время ожидания пересылки — время, в течение которого сервер пытается запросить сервер пересылки в случае отсутствия ответа. По истечении времени ожидания сервер пытается запросить следующий полномочный сервер из списка. Время ожидания по умолчанию — 5 секунд. Нажмите кнопку OK.
6. Повторите эту процедуру, чтобы настроить условную пересылку для других доменов.

Включение и отключение протоколирования событий

По умолчанию служба DNS отслеживает все DNS-события в журнале событий DNS-сервера. Записи этого журнала содержат информацию обо всех DNS-событиях и доступны через узел Просмотр событий в оснастке Управление компьютером. Это означает, что все информационные сообщения, предупреждения и ошибки будут записаны. Можно изменить параметры протоколирования так:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду Свойства.
2. Используйте параметры на вкладке Журнал событий (Event Logging). Чтобы отключить журналирование, установите переключатель не заносить никакие события (No Events).
3. Нажмите кнопку OK.

Использование журнала отладки для отслеживания активности DNS

Как правило, журнал событий DNS-сервер используется для наблюдения за деятельностью DNS-сервера. В этом журнале записаны все события DNS, а просмотреть его можно в узле Просмотр событий оснастки Управление компьютером. При поиске неисправностей DNS весьма полезной может оказаться настройка временного журнала для отслеживания определенных событий DNS. Не забудьте отключить события после окончания отладки. Для настройки отладки выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду Свойства.
2. Перейдите на вкладку Ведение журнала отладки (Debug Logging), установите флажок Записывать пакеты в журнал для отладки (Log packets for debugging), а затем отметьте флажки событий,

временное наблюдение за которыми необходимо вести. Используйте вкладку Ведение журнала отладки для выбора отслеживаемых событий
3. В поле Имя и путь к файлу (File path and name) введите имя файла журнала, например dns.log. По умолчанию журналы хранятся в папке %SystemRoot%\System32\Dns.
4. Нажмите кнопку OK. Завершив отладку, отключите протоколирование, сбросив флажок Записывать пакеты в журнал для отладки (Log packets for debugging).

Мониторинг DNS-сервера

В ОС Windows Server 2012 есть встроенная возможность мониторинга DNS-сервера. Эта процедура позволяет убедиться, что разрешение DNS имен настроено правильно. Чтобы настроить ручное или автоматическое выполнение мониторинга, выполните следующие действия:

1. В консоли Диспетчер DNS щелкните правой кнопкой мыши на сервере, который нужно настроить, и выберите команду Свойства.
2. Перейдите на вкладку Наблюдение (Monitoring) (рис. 16.12). Можно провести два типа тестов. Чтобы проверить разрешение DNS на текущем сервере, установите флажок Простой запрос к этому DNS-серверу (Simple query against this DNS server). Чтобы проверить разрешение DNS в домене, установите флажок Рекурсивный запрос к другим DNS-серверам (A recursive query to other DNS servers). Можно провести тестирование вручную. Для этого нажмите кнопку Тест (Test Now).
3. Чтобы запланировать автоматический мониторинг, установите флажок Автоматическое тестирование (Perform automatic testing at the following interval) и интервал в секундах, минутах или часах. Можно произвести ручное наблюдение или настроить сервер для автоматического мониторинга
4. Результаты тестирования отображаются в разделе Результаты теста (Test Results). Здесь указаны дата и время проведения теста, а также его результаты, например Пройден (Pass). Причиной отдельного сбоя может стать временная неисправность. Несколько сбоев указывают на проблему с разрешением имен.

Если провалены все рекурсивные тесты, нужно отключить рекурсию, выбрав опцию Отключить рекурсию (Disable Recursion) на вкладке Дополнительно.

Если данный момент диагностируется DNS, нужно производить тестирование каждые 10—15 секунд. Этот интервал обеспечивает быструю последовательность результатов теста. Если же просто нужно контролировать работу DNS, можете установить более длинный временной интервал, например два или три часа.

Литература

- Моримото Р., Ноэл М. Microsoft Windows Server 2012. Полное руководство. – М.:Вильямс, 2013. – 1456 с.: с ил.
- Станек У. Р. Microsoft Windows Server 2012. Справочник администратора. – М.:БВХ-Петербург, 2014, – 688 с.: с ил.
- Internet-ресурсы:
  www.microsoft.com/ru/ru/
  www.technet.microsoft.com/ru-ru
  www.citforum.ru
  www.intuit.ru
  www.wikipedia.org

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра аппаратно-программных комплексов вычислительной техники входит в состав Академии ЛИМТУ Университета ИТМО и имеет более чем 40-летний опыт научно-педагогической деятельности в области профессиональной переподготовки и повышения квалификации специалистов. За последние 20 лет на кафедре прошли обучение более 11 тысяч человек не только из Санкт-Петербурга, но и из различных городов России, а также стран ближнего и дальнего зарубежья. Наши выпускники работают руководителями проектов и начальниками IT-отделов, системными инженерами и системными администраторами, программистами и специалистами по эксплуатации аппаратно-программных комплексов вычислительной техники.

На сегодняшний день на кафедре реализуются следующие направления деятельности:

- подготовка магистров по направлению 09.04.01 «Информатика и вычислительная техника»;
- подготовка бакалавров (без отрыва от производства – вечерняя форма обучения) по направлению 09.03.01 Информатика и вычислительная техника;
- переподготовка специалистов, имеющих высшее образование, с выдачей государственного диплома о дополнительном (к высшему) образовании с присвоением квалификации;
- переподготовка специалистов, имеющих высшее и среднее профессиональное образование с выдачей государственного диплома о переподготовке с правом работы по новой специальности;
- повышение квалификации с выдачей государственного свидетельства (удостоверения)/сертификата Университета ИТМО.

С сентября 2003 года при кафедре функционирует Учебный центр, в котором проводится обучение по программным продуктам фирмы 1С последних версий.

С 2007 года на базе кафедры создан авторизованный Учебный центр фирмы ZyXEL, в котором проводится обучение по теории и практике применения современного сетевого оборудования для построения LAN-WAN сетей с использованием оборудования и технологий ZyXEL.

В 2012 году был создан Авторизованный Учебный центр фирмы QNAP для подготовки сертифицированных специалистов по системам IP-видеонаблюдения и сетевых хранилищ данных.

Программы обучения ориентированы на приобретение устойчивых профессиональных навыков и имеют практическую направленность. Основное время слушатели проводят за компьютером, выполняя большой объем практических заданий. Обучающиеся также получают минимальный объем теоретических знаний, необходимых для грамотного выполнения практических заданий.

Занятия проводятся в пяти специализированных классах, оснащенных современными компьютерами, объединенными в локальную вычислительную сеть с выходом в Интернет. Последние версии программных продуктов ведущих фирм производителей используются не только в учебном процессе, но и выдаются слушателям для установки на домашние компьютеры.

Постоянным заказчиком кафедры на переподготовку специалистов является Департамент федеральной государственной службы занятости населения по Санкт-Петербургу. Обучение слушателей осуществляется также на бюджетной и коммерческой основе.

Светлана Михайловна Платунова

Администрирование сети Windows Server 2012

Учебное пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж 100 экз.
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49